ISO/IEC 19896-2:2018 (E)

IT security techniques — Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Structure of this document

6 Knowledge

- 6.1 General
- 6.2 Tertiary education
- 6.2.1 General
- 6.2.2 Technical specialities
- 6.2.3 Speciality topics
- 6.3 Knowledge of standards
- 6.3.1 General
- 6.3.2 ISO/IEC 19790 concepts
- 6.3.3 ISO/IEC 24759
- 6.3.3.1 General
- 6.3.3.2 Vendor requirements
- 6.3.3.3 Test requirements
- 6.3.4 Additional ISO/IEC standards
- 6.4 Knowledge of the validation program
- 6.4.1 Validation program
- 6.4.1.1 General
- 6.4.1.2 Organization
- 6.4.1.3 Communications
- 6.4.1.4 Legal and regulatory mandates
- 6.4.1.5 Policies
- 6.4.1.6 Documentation
- 6.4.1.7 Tools
- 6.5 Knowledge of the requirements of ISO/IEC 17025

7 Skills

- 7.1 General
- 7.2 Algorithm testing
- 7.3 Physical security testing
- 7.4 Side channel analysis
- 7.5 Technology types

8 Experience

- 8.1 General
- 8.2 Demonstration of technical competence to the validation program
- 8.2.1 Experience with performing testing
- 8.2.2 Experience with particular technology types

9 Education

10 Effectiveness

Annex A (informative) Example of an ISO/IEC 24759 testers' log

Annex B (informative) Ontology of technology types and associated bodies of knowledge

B.1 General
B.2 Technology types
B.2.1 General
B.2.2 Software/firmware
B.2.2.1 Programming languages
B.2.2.2 Compilers
B.2.2.3 Debuggers or Simulators
B.2.2.4 Hardware
B.2.2.4.1 General knowledge
B.2.2.4.2 Single-chip modules
B.2.2.4.2.1 General knowledge about single-chip modules
B.2.2.4.2.2 Single-chip substrate materials
B.2.2.4.2.3 Single-chip packaging types
B.2.2.4.3 Multi-chip embedded modules
B.2.2.4.4 Multi-chip standalone modules

Annex C (informative) Specific knowledge associated with the security of cryptographic modules

C.1 General
C.2 Cryptographic module specification
C.2.1 General
C.2.2 Buffers
C.2.3 Security relevant components
C.2.4 Identification of programmable interfaces, debugging interfaces and covert channels
C.2.5 Identification of approved and non-approved security functions
C.2.6 Exclusion of components
C.2.7 Degraded operation
C.3 Cryptographic module interfaces
C.3.1 Overview
C.3.2 Separation of input data from output data
C.3.3 Knowledge of critical security functions, services or security relevant services
C.3.4 Trusted channel
C.4 Roles, services, and authentication
C.4.1 General
C.4.2 Services
C.4.3 Authentication
C.5 Software/firmware security
C.6 Operational environment
C.6.1 Process memory management
C.6.2 Loading
C.6.3 Linking
C.6.4 Virtual memory
C.7 Physical security
C.8 Non-invasive security
C.9 Sensitive security parameter management
C.9.1 General
C.9.2 Password vs cryptographic key
C.9.3 Entropy vs attackers' knowledge
C.9.4 SSP hierarchy
C.9.4.1 General
C.9.4.2 Split knowledge
C.9.5 Authorized roles for SSPs management
C.9.6 Zeroization
C.9.6.1 Copies of SSPs
C.9.6.2 Embodiment of storage device
C.9.6.2.1 Flash memory
C.9.6.2.2 Hard disk drive

C.10 Self-tests
C.10.1 General
C.10.2 Critical functions
C.10.2.1 Notion of critical functions
C.10.2.2 Pre-defined critical functions
C.10.2.3 Vendor-defined critical functions
C.10.3 Pre-operational software/firmware integrity test
C.10.3.1 Scope of pre-operational software/firmware integrity test
C.10.3.2 Use of a truncated version of approved message authentication code
C.10.3.3 Single encompassing message authentication code vs multiple disjoint codes
C.10.4 Conditional cryptographic algorithm self-tests
C.10.5 Pair-wise consistency test
C.11 Life-cycle assurance
C.11.1 General
C.11.2 Configuration management
C.11.3 Finite state model
C.11.3.1 Minimum resolution of states
C.11.3.2 Definition of error states
C.11.4 Development
C.11.4.1 Mapping to finite state model
C.11.4.2 Tools and automation
C.11.4.3 Unnecessary code, parameters and symbols
C.11.4.4 Pre-conditions and post-conditions
C.11.5 Vendor testing
C.11.5.1 General
C.11.5.2 Low-level testing
C.11.6 Delivery and operation
C.11.7 End of life
C.11.8 Guidance documents
C.12 Mitigation of other attacks

Annex D (informative) Competence requirements for ISO/IEC 19790 validators

Page count: 34