ISO/IEC TS 19249:2017-10 (E)

Information technology - Security techniques - Catalogue of architectural and design principles for secure products, systems and applications

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Architectural principles for secure products, systems and applications 2
4.1 General 2
4.2 Domain separation 3
4.2.1 General 3
4.2.2 Principles for defining domain structures 3
4.2.3 Principles for defining inter-domain communication 3
4.2.4 Security policies that may be enforced using domain separation 4
4.2.5 Examples 4
4.2.6 Considerations for evaluation 4
4.3 Layering 5
4.3.1 General 5
4.3.2 Principles for defining layers 5
4.3.3 Principles for Interfaces exposed by a layer 5
4.3.4 Security policies that may be enforced using layering 5
4.3.5 Examples 6
4.3.6 Considerations for evaluation 6
4.4 Encapsulation 6
4.4.1 General 6
4.4.2 Principles for defining encapsulation 7
4.4.3 Security policies that may be enforced using encapsulation 7
4.4.4 Examples 7
4.4.5 Considerations for evaluation 7
4.5 Redundancy 7
4.5.1 General 7
4.5.2 Principles for defining redundant elements 8
4.5.3 Principles for keeping consistency between redundant elements 8
4.5.4 Security policies that may be enforced using redundancy 8
4.5.5 Examples 8
4.5.6 Considerations for evaluation 9
4.6 Virtualization 10
4.6.1 General 10
4.6.2 Principles for defining virtualization 10
4.6.3 Security policies that may be enforced using virtualization 10
4.6.4 Examples 11
4.6.5 Considerations for evaluation 11

5 Design principles 11
5.1 General 11
5.2 List of design principles for security 12
5.2.1 Least privilege 12
5.2.2 Attack surface minimization 13

5.2.3 Centralized parameter validation 15
5.2.4 Centralized general security services 17
5.2.5 Preparing for error and exception handling 18
5.3 Using the design principles when designing a secure system or application 20
5.3.1 General 20
5.3.2 Least privilege 20
5.3.3 Attack surface minimization 20
5.3.4 Centralized parameter validation 20
5.3.5 Centralized security services 20
5.3.6 Preparing for error and exception handling 21

6 Evaluation activities for the architectural principles 21
6.1 General 21
6.2 Domain separation 22
6.3 Layering 23
6.4 Encapsulation 23
6.5 Redundancy 24
6.6 Virtualization 25

Bibliography 26