

ISO/IEC 18045:2008-08 (E)

Information technology - Security techniques - Methodology for IT security evaluation

Contents		Page
Foreword		vii
Introduction		ix
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	Overview	3
5.1	Organisation of this International Standard	3
6	Document Conventions	3
6.1	Terminology	3
6.2	Verb usage	3
6.3	General evaluation guidance	4
7	Evaluation process and related tasks	5
7.1	Introduction	5
7.2	Evaluation process overview	5
7.2.1	Objectives	5
7.2.2	Responsibilities of the roles	5
7.2.3	Relationship of roles	6
7.2.4	General evaluation model	6
7.2.5	Evaluator verdicts	6
7.3	Evaluation input task	8
7.3.1	Objectives	8
7.3.2	Application notes	8
7.3.3	Management of evaluation evidence sub-task	8
7.4	Evaluation sub-activities	9
7.5	Evaluation output task	9
7.5.1	Objectives	9
7.5.2	Management of evaluation outputs	9
7.5.3	Application notes	10
7.5.4	Write OR sub-task	10
7.5.5	Write ETR sub-task	10
8	Class APE: Protection Profile evaluation	15
8.1	Introduction	15
8.2	Application notes	16
8.2.1	Re-using the evaluation results of certified PPs	16
8.3	PP introduction (APE_INT)	16
8.3.1	Evaluation of sub-activity (APE_INT.1)	16
8.4	Conformance claims (APE_CCL)	17
8.4.1	Evaluation of sub-activity (APE_CCL.1)	17
8.5	Security problem definition (APE_SPD)	24
8.5.1	Evaluation of sub-activity (APE_SPD.1)	24
8.6	Security objectives (APE_OBJ)	25

8.6.1	Evaluation of sub-activity (APE_OBJ.1)	25
8.6.2	Evaluation of sub-activity (APE_OBJ.2)	25
8.7	Extended components definition (APE_ECD)	28
8.7.1	Evaluation of sub-activity (APE_ECD.1)	28
8.8	Security requirements (APE_REQ)	31
8.8.1	Evaluation of sub-activity (APE_REQ.1)	31
8.8.2	Evaluation of sub-activity (APE_REQ.2)	35
9	Class ASE: Security Target evaluation	39
9.1	Introduction	39
9.2	Application notes	39
9.2.1	Re-using the evaluation results of certified PPs	39
9.3	ST introduction (ASE_INT)	39
9.3.1	Evaluation of sub-activity (ASE_INT.1)	39
9.4	Conformance claims (ASE_CCL)	42
9.4.1	Evaluation of sub-activity (ASE_CCL.1)	42
9.5	Security problem definition (ASE_SPD)	49
9.5.1	Evaluation of sub-activity (ASE_SPD.1)	49
9.6	Security objectives (ASE_OBJ)	51
9.6.1	Evaluation of sub-activity (ASE_OBJ.1)	51
9.6.2	Evaluation of sub-activity (ASE_OBJ.2)	51
9.7	Extended components definition (ASE_ECD)	53
9.7.1	Evaluation of sub-activity (ASE_ECD.1)	53
9.8	Security requirements (ASE_REQ)	57
9.8.1	Evaluation of sub-activity (ASE_REQ.1)	57
9.8.2	Evaluation of sub-activity (ASE_REQ.2)	60
9.9	TOE summary specification (ASE_TSS)	64
9.9.1	Evaluation of sub-activity (ASE_TSS.1)	64
9.9.2	Evaluation of sub-activity (ASE_TSS.2)	65
10	Class ADV: Development	67
10.1	Introduction	67
10.2	Application notes	67
10.3	Security Architecture (ADV_ARC)	67
10.3.1	Evaluation of sub-activity (ADV_ARC.1)	67
10.4	Functional specification (ADV_FSP)	72
10.4.1	Evaluation of sub-activity (ADV_FSP.1)	72
10.4.2	Evaluation of sub-activity (ADV_FSP.2)	75
10.4.3	Evaluation of sub-activity (ADV_FSP.3)	79
10.4.4	Evaluation of sub-activity (ADV_FSP.4)	84
10.4.5	Evaluation of sub-activity (ADV_FSP.5)	89
10.4.6	Evaluation of sub-activity (ADV_FSP.6)	94
10.5	Implementation representation (ADV_IMP)	95
10.5.1	Evaluation of sub-activity (ADV_IMP.1)	95
10.5.2	Evaluation of sub-activity (ADV_IMP.2)	97
10.6	TSF internals (ADV_INT)	97
10.6.1	Evaluation of sub-activity (ADV_INT.1)	97
10.6.2	Evaluation of sub-activity (ADV_INT.2)	99
10.6.3	Evaluation of sub-activity (ADV_INT.3)	101
10.7	Security policy modelling (ADV_SPM)	101
10.7.1	Evaluation of sub-activity (ADV_SPM.1)	101
10.8	TOE design (ADV_TDS)	101
10.8.1	Evaluation of sub-activity (ADV_TDS.1)	101
10.8.2	Evaluation of sub-activity (ADV_TDS.2)	105
10.8.3	Evaluation of sub-activity (ADV_TDS.3)	109
10.8.4	Evaluation of sub-activity (ADV_TDS.4)	118
10.8.5	Evaluation of sub-activity (ADV_TDS.5)	126
10.8.6	Evaluation of sub-activity (ADV_TDS.6)	126
11	Class AGD: Guidance documents	127
11.1	Introduction	127
11.2	Application notes	127

11.3	Operational user guidance (AGD_OPE)	127
11.3.1	Evaluation of sub-activity (AGD_OPE.1)	127
11.4	Preparative procedures (AGD_PRE)	130
11.4.1	Evaluation of sub-activity (AGD_PRE.1)	130
12	Class ALC: Life-cycle support	131
12.1	Introduction	131
12.2	CM capabilities (ALC_CMC)	132
12.2.1	Evaluation of sub-activity (ALC_CMC.1)	132
12.2.2	Evaluation of sub-activity (ALC_CMC.2)	133
12.2.3	Evaluation of sub-activity (ALC_CMC.3)	135
12.2.4	Evaluation of sub-activity (ALC_CMC.4)	138
12.2.5	Evaluation of sub-activity (ALC_CMC.5)	143
12.3	CM scope (ALC_CMS)	150
12.3.1	Evaluation of sub-activity (ALC_CMS.1)	150
12.3.2	Evaluation of sub-activity (ALC_CMS.2)	151
12.3.3	Evaluation of sub-activity (ALC_CMS.3)	152
12.3.4	Evaluation of sub-activity (ALC_CMS.4)	153
12.3.5	Evaluation of sub-activity (ALC_CMS.5)	154
12.4	Delivery (ALC_DEL)	155
12.4.1	Evaluation of sub-activity (ALC_DEL.1)	155
12.5	Development security (ALC_DVS)	156
12.5.1	Evaluation of sub-activity (ALC_DVS.1)	156
12.5.2	Evaluation of sub-activity (ALC_DVS.2)	158
12.6	Flaw remediation (ALC_FLR)	161
12.6.1	Evaluation of sub-activity (ALC_FLR.1)	161
12.6.2	Evaluation of sub-activity (ALC_FLR.2)	163
12.6.3	Evaluation of sub-activity (ALC_FLR.3)	167
12.7	Life-cycle definition (ALC_LCD)	171
12.7.1	Evaluation of sub-activity (ALC_LCD.1)	171
12.7.2	Evaluation of sub-activity (ALC_LCD.2)	172
12.8	Tools and techniques (ALC_TAT)	174
12.8.1	Evaluation of sub-activity (ALC_TAT.1)	174
12.8.2	Evaluation of sub-activity (ALC_TAT.2)	176
12.8.3	Evaluation of sub-activity (ALC_TAT.3)	178
13	Class ATE: Tests	181
13.1	Introduction	181
13.2	Application notes	181
13.2.1	Understanding the expected behaviour of the TOE	181
13.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality	182
13.2.3	Verifying the adequacy of tests	182
13.3	Coverage (ATE_COV)	183
13.3.1	Evaluation of sub-activity (ATE_COV.1)	183
13.3.2	Evaluation of sub-activity (ATE_COV.2)	183
13.3.3	Evaluation of sub-activity (ATE_COV.3)	184
13.4	Depth (ATE_DPT)	185
13.4.1	Evaluation of sub-activity (ATE_DPT.1)	185
13.4.2	Evaluation of sub-activity (ATE_DPT.2)	187
13.4.3	Evaluation of sub-activity (ATE_DPT.3)	189
13.4.4	Evaluation of sub-activity (ATE_DPT.4)	192
13.5	Functional tests (ATE_FUN)	192
13.5.1	Evaluation of sub-activity (ATE_FUN.1)	192
13.5.2	Evaluation of sub-activity (ATE_FUN.2)	195
13.6	Independent testing (ATE_IND)	195
13.6.1	Evaluation of sub-activity (ATE_IND.1)	195
13.6.2	Evaluation of sub-activity (ATE_IND.2)	198
13.6.3	Evaluation of sub-activity (ATE_IND.3)	203
14	Class AVA: Vulnerability assessment	203
14.1	Introduction	203
14.2	Vulnerability analysis (AVA_VAN)	204

14.2.1	Evaluation of sub-activity (AVA_VAN.1)	204
14.2.2	Evaluation of sub-activity (AVA_VAN.2)	208
14.2.3	Evaluation of sub-activity (AVA_VAN.3)	215
14.2.4	Evaluation of sub-activity (AVA_VAN.4)	222
14.2.5	Evaluation of sub-activity (AVA_VAN.5)	230
15	Class ACO: Composition	230
15.1	Introduction	230
15.2	Application notes	230
15.3	Composition rationale (ACO_COR)	231
15.3.1	Evaluation of sub-activity (ACO_COR.1)	231
15.4	Development evidence (ACO_DEV)	236
15.4.1	Evaluation of sub-activity (ACO_DEV.1)	236
15.4.2	Evaluation of sub-activity (ACO_DEV.2)	237
15.4.3	Evaluation of sub-activity (ACO_DEV.3)	239
15.5	Reliance of dependent component (ACO_REL)	242
15.5.1	Evaluation of sub-activity (ACO_REL.1)	242
15.5.2	Evaluation of sub-activity (ACO_REL.2)	244
15.6	Composed TOE testing (ACO_CTT)	246
15.6.1	Evaluation of sub-activity (ACO_CTT.1)	246
15.6.2	Evaluation of sub-activity (ACO_CTT.2)	248
15.7	Composition vulnerability analysis (ACO_VUL)	252
15.7.1	Evaluation of sub-activity (ACO_VUL.1)	252
15.7.2	Evaluation of sub-activity (ACO_VUL.2)	254
15.7.3	Evaluation of sub-activity (ACO_VUL.3)	258
Annex A (informative) General evaluation guidance		262
A.1	Objectives	262
A.2	Sampling	262
A.3	Dependencies	264
A.3.1	Dependencies between activities	264
A.3.2	Dependencies between sub-activities	264
A.3.3	Dependencies between actions	264
A.4	Site Visits	264
A.4.1	Introduction	264
A.4.2	General Approach	265
A.4.3	Orientation Guide for the Preparation of the Check List	266
A.4.4	Example of a checklist	267
A.5	Scheme Responsibilities	269
Annex B (informative) Vulnerability Assessment (AVA)		271
B.1	What is Vulnerability Analysis	271
B.2	Evaluator construction of a Vulnerability Analysis	271
B.2.1	Generic vulnerability guidance	272
B.2.2	Identification of Potential Vulnerabilities	279
B.3	When attack potential is used	281
B.3.1	Developer	281
B.3.2	Evaluator	282
B.4	Calculating attack potential	283
B.4.1	Application of attack potential	283
B.4.2	Characterising attack potential	283
B.5	Example calculation for direct attack	289