

ISO/IEC 29128:2011-12 (E)

Information technology - Security techniques - Verification of cryptographic protocols

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Terms and definitions	1
3	Symbols and notation	2
4	General	3
5	Specifying cryptographic protocols	5
5.1	Objectives	5
5.2	The abstraction levels	5
5.3	The specification of security protocols	5
5.3.1	General	5
5.3.2	The symbolic messages	5
5.3.3	Observing messages	6
5.3.4	Algebraic properties	7
5.3.5	Protocol roles	7
5.4	The specification of adversarial model	8
5.4.1	Network specification	8
5.4.2	The attacker	8
5.4.3	The scenario	9
5.5	The specification of security properties	10
5.5.1	General	10
5.5.2	Trace properties	11
6	Cryptographic protocol assurance levels	12
6.1	General	12
6.2	Protocol Assurance Level 1	13
6.3	Protocol Assurance Level 2	13
6.4	Protocol Assurance Level 3	14
6.5	Protocol Assurance Level 4	14
6.6	Difference among Protocol Assurance Levels	14
7	Security Assessment and Verification	16
7.1	Protocol specification	16
7.1.1	PPS_SEMIFORMAL	16
7.1.2	PPS_FORMAL	17
7.1.3	PPS_MECHANIZED	17
7.2	Adversarial model	18
7.2.1	PAM INFORMAL	18
7.2.2	PAM_FORMAL	18
7.2.3	PAM_MECHANIZED	19
7.3	Security properties	20
7.3.1	General	20
7.3.2	PSP_INFORMAL	21
7.3.3	PSP_FORMAL	21
7.3.4	PSP_MECHANIZED	22

7.4	Self-assessment evidence for verification	23
7.4.1	General	23
7.4.2	PEV_ARGUMENT	23
7.4.3	PEV_HANDPROVEN	23
7.4.4	PEV_BOUNDED	24
7.4.5	PEV_UNBOUNDED	24
8	Common Methodology for Cryptographic Protocols Security Evaluation	25
8.1	Introduction	25
8.2	Protocol specification evaluation	26
8.2.1	Evaluation of sub-activity (PPS_SEMIFORMAL)	26
8.2.2	Evaluation of sub-activity (PPS_FORMAL)	26
8.2.3	Evaluation of sub-activity (PPS_MECHANIZED)	26
8.3	Adversarial model evaluation	27
8.3.1	Evaluation of sub-activity (PAM INFORMAL)	27
8.3.2	Evaluation of sub-activity (PAM_FORMAL)	27
8.3.3	Evaluation of sub-activity (PAM_MECHANIZED)	28
8.4	Security properties evaluation	28
8.4.1	Evaluation of sub-activity (PSP_INFORMAL)	28
8.4.2	Evaluation of sub-activity (PSP_FORMAL)	28
8.4.3	Evaluation of sub-activity (PSP_MECHANIZED)	29
8.5	Self-assessment evidence evaluation	29
8.5.1	Evaluation of sub-activity (PEV_ARGUMENT)	29
8.5.2	Evaluation of sub-activity (PEV_HANDPROVEN)	30
8.5.3	Evaluation of sub-activity (PEV_BOUNDED)	30
8.5.4	Evaluation of sub-activity (PEV_UNBOUNDED)	30
	Annex A (informative) Guidelines for Cryptographic Protocol Design	32
	Annex B (informative) Example of formal specification	34
B.1	Symbolic specification of security protocols	34
B.1.1	Abstraction level	34
B.1.2	Protocol specifications	35
B.2	State transitions	37
B.2.1	Attacker model	37
B.2.2	Configuration state	37
B.2.3	Traces	38
B.3	Trace properties	38
B.3.1	Secrecy	38
B.3.2	Authentication	39
	Annex C (informative) Verification examples	41
C.1	Sample protocol	41
C.2	Design artifacts	41
C.2.1	Input to protocol verification tool	42
C.2.2	Protocol Specification	43
C.2.3	Operating Environment	44
C.2.4	Security Properties	44
C.2.5	Evidence	44
C.3	Additional inputs for verification	47
	Bibliography	49