

Informační technologie – Bezpečnostní techniky – Verifikace kryptografických protokolů
ČSN
ISO/IEC 29128
36 9707

Information technology – Security techniques – Verification of cryptographic protocols

Technologies de l'information – Techniques de sécurité – Vérification des protocoles cryptographiques

Tato norma je českou verzí mezinárodní normy ISO/IEC 29128:2011. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29128:2011. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Souvisící ČSN

ČSN ISO/IEC 15408-1:2013 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ČSN ISO/IEC 15408-2:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ČSN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původním tvaru, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu: nonce, man-in-the-middle.

Anglický termín „seed“ je přeložen jako „náhodná počáteční hodnota“.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 29128

Verifikace kryptografických protokolů První vydání

2011-12-15

ICS 35.040

Obsah

Strana

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Termíny a definice 8

3 Symboly a způsob zápisu 9

4 Obecně 9

5 Specifikování kryptografických protokolů 10

5.1 Cíle 10

5.2 Úrovně abstrakce 10

5.3 Specifikace bezpečnostních protokolů 10

5.3.1 Obecně 10

5.3.2 Symbolické zprávy 10

5.3.3 Zprávy založené na pozorování 11

5.3.4 Algebraické vlastnosti 11

5.3.5 Role protokolů 11

5.4 Specifikace modelu protivníka 12

5.4.1 Specifikace sítě 12

5.4.2 Útočník 12

5.4.3 Scénář 13

5.5	Specifikace bezpečnostních vlastností	13
5.5.1	Obecně	13
5.5.2	Vlastnosti stopy	14
6	Úrovně záruky kryptografických protokolů	14
6.1	Obecně	14
6.2	Úroveň 1 záruky protokolu	15
6.3	Úroveň 2 záruky protokolu	15
6.4	Úroveň 3 záruky protokolu	15
6.5	Úroveň 4 záruky protokolu	15
6.6	Rozdíl mezi úrovněmi záruky protokolu	16
6.7	Odpovídající úrovně záruky v ISO/IEC 15408	16
7	Posouzení a verifikace bezpečnosti	17
7.1	Specifikace protokolu	17
7.1.1	PPS_SEMIFORMAL	17
7.1.2	PPS_FORMAL	17
7.1.3	PPS_MECHANIZED	18
7.2	Model protivníka	18
7.2.1	PAM_INFORMAL	18
7.2.2	PAM_FORMAL	18
7.2.3	PAM_MECHANIZED	19
7.3	Bezpečnostní vlastnosti	19
7.3.1	Obecně	19
7.3.2	PSP_INFORMAL	20
7.3.3	PSP_FORMAL	20
7.3.4	PSP_MECHANIZED	20
7.4	Sebehodnotící důkaz pro verifikaci	21
7.4.1	Obecně	21

7.4.2	PEV_ARGUMENT	21
7.4.3	PEV_HANDPROVEN	21
7.4.4	PEV_BOUNDED	22
7.4.5	PEV_UNBOUNDED	22
8	Obecná metodika pro hodnocení bezpečnosti kryptografických protokolů	23
8.1	Úvod	23
8.2	Hodnocení specifikace protokolu	23
8.2.1	Hodnocení subaktivity (PPS_SEMIFORMAL)	23
8.2.2	Hodnocení subaktivity (PPS_FORMAL)	23
8.2.3	Hodnocení subaktivity (PPS_MECHANIZED)	23
8.3	Hodnocení modelu protivníka	23
8.3.1	Hodnocení subaktivity (PAM_INFORMAL)	23
8.3.2	Hodnocení subaktivity (PAM_FORMAL)	24
8.3.3	Hodnocení subaktivity (PAM_MECHANIZED)	24
8.4	Hodnocení bezpečnostních vlastností	24
8.4.1	Hodnocení subaktivity (PSP_INFORMAL)	24
8.4.2	Hodnocení subaktivity (PSP_FORMAL)	24
8.4.3	Hodnocení subaktivity (PSP_MECHANIZED)	25
8.5	Hodnocení důkazu sebeposuzování	25
8.5.1	Hodnocení subaktivity (PEV_ARGUMENT)	25
8.5.2	Hodnocení subaktivity (PEV_HANDPROVEN)	25
8.5.3	Hodnocení subaktivity (PEV_BOUNDED)	25
8.5.4	Hodnocení subaktivity (PEV_UNBOUNDED)	26
Příloha A	(informativní) Směrnice pro návrh kryptografického protokolu	27
Příloha B	(informativní) Příklad formální specifikace	28
B.1	Symbolická specifikace bezpečnostních protokolů	28
B.1.1	Abstraktní úroveň	28
B.1.2	Specifikace protokolu	29

B.2 Přechodové stavy 29

B.2.1 Model útočníka 29

Strana

B.2.2 Stav konfigurace 30

B.2.3 Stopy 30

B.3 Vlastnosti stop 30

B.3.1 Utajení 30

B.3.2 Autentizace 31

Příloha C (informativní) Příklady verifikace 32

C.1 Vzorový protokol 32

C.2 Artefakty návrhu 32

C.2.1 Vstup do nástroje na verifikaci protokolu 32

C.2.2 Specifikace protokolu 34

C.2.3 Provozní prostředí 34

C.2.4 Bezpečnostní vlastnosti 34

C.2.5 Důkaz 35

C.3 Další vstupy pro verifikaci 36

Bibliografie 38

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2011

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoli nebo všech patentových práv.

ISO/IEC 29128 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Bezpečnost digitální komunikace závisí na mnoha aspektech, kdy kryptografické mechanismy hrají stále důležitější roli. Jsou-li takové mechanismy používány, existuje mnoho bezpečnostních záležitostí, jako jsou síla kryptografických algoritmů, přesnost a správnost implementace, správná činnost a použití kryptografických systémů, a bezpečnost nasazených kryptografických protokolů.

Normy pro specifikaci kryptografických algoritmů a pro implementaci a testování kryptografických zařízení a modulů již existují. Neexistují však žádné normy nebo obecněji akceptované postupy pro posuzování specifikace protokolů použitých v takové komunikaci. Cílem této mezinárodní normy je ustavit prostředky pro verifikaci specifikací kryptografických protokolů a poskytnout tak definované úrovně důvěry týkající se bezpečnosti specifikace kryptografických protokolů.

1 Předmět normy

Tato mezinárodní norma stanoví technický základ pro bezpečnostní důkaz specifikace kryptografických protokolů. Tato mezinárodní norma specifikuje kritéria hodnocení návrhu pro tyto protokoly, stejně jako metody, určené k použití v procesu verifikace takových protokolů. Tato mezinárodní norma také poskytuje definice různých úrovní záruky protokolů odpovídajících komponentám záruky hodnocení v ISO/IEC 15408.

Konec náhledu - text dále pokračuje v placené verzi ČSN.