

2022

Bezpečnost informací – Kritéria a metodika
pro hodnocení bezpečnosti biometrických systémů –
Část 3: Detekce prezentačního útoku

ČSN
ISO/IEC 19989-3

36 9859

Information security – Criteria and methodology for security evaluation of biometric systems –
Part 3: Presentation attack detection

Sécurité de l'information – Critères et méthodologie pour l'évaluation de la sécurité des systèmes
biométriques –
Partie 3: Détection d'attaque de présentation

Tato norma je českou verzí mezinárodní normy ISO/IEC 19989-3:2020. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 19989-3:2020. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 15408-3:2008 zavedena v ČSN EN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ISO/IEC 18045:2008 zavedena v ČSN EN ISO/IEC 18045:2020 (36 9805) Informační technologie – Bezpečnostní techniky – Metodika pro hodnocení bezpečnosti IT

ISO/IEC 19989-1:2020 zavedena v ČSN ISO/IEC 19989-1:2021 (36 9859) Bezpečnost informací – Kritéria a metodika pro hodnocení bezpečnosti biometrických systémů – Část 1: Rámec

ISO/IEC 30107-3:2017 zavedena v ČSN ISO/IEC 30107-3:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 3: Testování a podávání zpráv

Souvisící ČSN

ČSN ISO/IEC 2382-37:2018 (36 9001) Informační technologie – Slovník – Část 37: Biometrika

ČSN EN 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 19792:2016 (36 9858) Informační technologie – Bezpečnostní techniky – Hodnocení bezpečnosti biometrie

ČSN ISO/IEC 30107-1:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

Vypracování normy

Zpracovatel: Prof. Ing., Dipl. Ing. Martin Drahanský, Ph.D., IČO 73840602

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.030

Obsah

Strana

Předmluva.....	
.....	5
Úvod.....	
.....	6
1..... Předmět normy.....	
.....	7
2..... Citované dokumenty.....	
.....	7
3..... Termíny a definice.....	
.....	7
4..... Zkratky a zkrácené termíny.....	
.....	10
5..... Obecná poznámka.....	
.....	11
6..... Přehled testování PAD ve třídě ATE a ve třídě AVA.....	11
6.1..... Cíle a principy.....	
.....	11
6.1.1... Třída ATE.....	
.....	11
6.1.2... Třída AVA.....	

.....	11
6.2..... PAI použité v testovacích aktivitách.....	12
6.2.1... Třída ATE.....	12
6.2.2... Třída AVA.....	12
6.3..... Testovací aktivity.....	12
6.3.1... Třída ATE.....	12
6.3.2... Třída AVA.....	12
6.4..... Kritéria úspěchu/neúspěchu.....	13
7..... Doplnkové činnosti k ISO/IEC 18045 o testech (ATE).....	13
7.1..... Testovací přístup k PAD.....	13
7.2..... Metriky pro testování PAD.....	13
7.2.1... Obecně.....	13
7.2.2... Metriky používané pro TOE subsystému PAD.....	14
7.2.3... Metriky používané pro TOE subsystému pro zachycení dat.....	14
7.2.4... Metriky používané pro jiné TOE.....	15

7.3..... Minimální velikosti testů a maximální chybové míry.....	15
8..... Doplnkové aktivity k ISO/IEC 18045 o posouzení zranitelnosti (AVA).....	16
8.1..... Penetrační testování pomocí variací PAI.....	16
8.2..... Potenciální zranitelnosti.....	17
8.3..... Hodnocení zranitelnosti a odolnosti TOE.....	17
Příloha A (informativní) Příklady výpočtů potenciálu útoku.....	18
Bibliografie	23



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2020

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopii nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

CP 401 · Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Tel.: + 41 22 749 01 11

E-mail: copyright@iso.org

Web: www.iso.org

Publikováno ve Švýcarsku

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržných ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí*.

Seznam všech částí souboru ISO/IEC 19989 lze nalézt na webových stránkách ISO.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

Biometrické systémy mohou být zranitelné vůči prezentačním útokům, kdy se útočníci pokoušejí rozvrátit bezpečnostní politiku systému tím, že prezentují své přirozené biometrické charakteristiky nebo artefakty obsahující kopírované nebo předstírané vlastnosti. K prezentačním útokům může dojít během událostí registrace nebo identifikace/ověření. Techniky určené k detekci prezentačních artefaktů se obecně liší od technik odvrácení útoků, kde se používají přirozené charakteristiky. Ochrana před prezentačními útoky s přirozenými charakteristikami se obvykle spoléhá na schopnost biometrického systému rozlišovat mezi oprávněnými registrovanými subjekty a útočníky na základě rozdílů mezi jejich přirozenými biometrickými charakteristikami. Tato schopnost je charakterizována výkonností biometrického rozpoznávání systému. Výkonnost biometrického rozpoznávání a detekce prezentačního útoku mají vliv na bezpečnost biometrických systémů. Hodnocení těchto aspektů výkonnosti z hlediska bezpečnosti se proto stane důležitým faktorem při pořizování biometrických produktů a systémů.

Biometrické produkty a systémy sdílejí mnoho vlastností jiných produktů a systémů IT, u kterých se k hodnocení bezpečnosti z pohledu normalizace využívá soubor ISO/IEC 15408 a ISO/IEC 18045. Biometrické systémy však ztělesňují určité funkce, které vyžadují specializovaná hodnotící kritéria a metodiku, která nejsou řešena v souboru ISO/IEC 15408 ani v ISO/IEC 18045. Tyto se týkají především hodnocení biometrického rozpoznávání a detekce prezentačního útoku. To jsou funkce, kterým se věnuje tento dokument.

ISO/IEC 19792 popisuje tyto biometrické aspekty a specifikuje principy, které je třeba vzít v úvahu při hodnocení bezpečnosti biometrických systémů. Nespecifikuje však konkrétní kritéria a metodiku, které jsou nutné pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408.

Soubor ISO/IEC 19989 představuje most mezi principy hodnocení biometrických produktů a systémů definovaných v ISO/IEC 19792 a kritérii a metodickými požadavky pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408. Soubor ISO/IEC 19989 doplňuje soubor ISO/IEC 15408 a ISO/IEC 18045 tím, že poskytuje rozšířené bezpečnostní funkční požadavky spolu s činnostmi záruk souvisícími s těmito požadavky. Rozšíření požadavků a činnostmi záruk nalezených v souboru ISO/IEC 15408 a v ISO/IEC 18045 souvisí s hodnocením biometrického rozpoznávání a detekcí prezentačního útoku, které se týkají zejména biometrických systémů.

Tento dokument poskytuje návod a požadavky pro vývojáře a hodnotitele pro doplňkové činnosti týkající se detekce prezentačního útoku specifikované v ISO/IEC 19989-1. Navazuje na obecné úvahy popsané v ISO/IEC 19792 a na metodiku testování detekce prezentačního útoku popsanou v ISO/IEC 30107-3 tím, že poskytuje hodnotiteli další návod.

V tomto dokumentu se termín „uživatel“ používá ve významu termínu „zachycený subjekt“, který se používá v biometrice.

1 Předmět normy

Pro hodnocení bezpečnosti systémů biometrického ověření a systémů biometrické identifikace se tento dokument věnuje bezpečnostnímu hodnocení detekce prezentačního útoku s využitím souboru ISO/IEC 15408. Poskytuje doporučení a požadavky pro vývojáře a hodnotitele pro doplňkové aktivity týkající se detekce prezentačního útoku specifikované v ISO/IEC 19989-1.

Tento dokument je použitelný pouze pro TOE pro jeden typ biometrické charakteristiky, ale pro volbu charakteristiky z více charakteristik.

Konec náhledu - text dále pokračuje v placené verzi ČSN.