

2025

Informační technologie – Detekce biometrického
prezentačního útoku –
Část 4: Profil pro testování v mobilních zařízeních

ČSN
ISO/IEC 30107-4

36 9862

Information technology – Biometric presentation attack detection –
Part 4: Profile for testing of mobile devices

Technologies de l'information – Détection d'attaque de présentation en biométrie –
Partie 4: Profil pour les essais des dispositifs mobiles

Tato norma je českou verzí mezinárodní normy ISO/IEC 30107-4:2024. 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 30107-4:2024. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 30107-4 (36 9862) z dubna 2021.

Národní předmluva

Změny proti předchozí normě

Norma je technickou revizí předchozího vydání. Podrobnosti o změnách jsou uvedeny v předmluvě k mezinárodní normě.

Informace o citovaných dokumentech

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

ISO/IEC 19795-1 zavedena v ČSN ISO/IEC 19795-1 (36 9861) Informační technologie – Testování biometrické výkonnosti a podávání zpráv – Část 1: Principy a rámec

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

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

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „Informace o citovaných dokumentech“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

Vypracování normy

Zpracovatel odborného překladu: Prof. Ing., Dipl.-Ing. Martin Dražanský, Ph.D., IČO 73840602

Technická normalizační komise: TNK 42 Výměna dat

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

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 35.240.15

Obsah

Strana

Předmluva..... 4

Úvod..... 5

1..... Předmět
normy..... 6

2..... Citované
dokumenty..... 6

3..... Termíny
a definice..... 6

4.....
Zkratky..... 7

5.....
Shoda..... 7

6..... Obecný profil pro testování PAD v mobilních
zařízeních..... 7

7..... Profil FIDO pro testování PAD v mobilních
zařízeních..... 12

Bibliografie..... 16



© ISO/IEC 2024

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 fotokopíí 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) 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 oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

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 nebo www.iec.ch/members_experts/refdocs).

ISO a IEC upozorňují na možnost, že implementace tohoto dokumentu smí vyžadovat využití patentu (patentů). V souvislosti s tím ISO a IEC nezaujímají žádné stanovisko týkající se důkazů, platnosti nebo použitelnosti všech uplatňovaných patentových práv. Ke dni zveřejnění tohoto dokumentu ISO a IEC neobdržely oznámení o patentu (patentech), který smí být vyžadován pro implementaci tohoto dokumentu. ISO a IEC však upozorňují implementující organizace, že se nemusí jednat o nejnovější informace, které lze získat z databáze patentů dostupné na www.iso.org/patents a [https://patents.iec.ch](http://patents.iec.ch). ISO a IEC nelze činit odpovědné za identifikaci jakéhokoliv nebo všech takových patentových práv.

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená 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), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 37 *Biometrika*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 30107-4:2020), které bylo technicky zrevidováno.

Hlavní změny jsou:

- odstranění termínů a definic obsažených v jiných částech souboru ISO/IEC 30107;
- doplnění biometrických požadavků FIDO;
- doplnění kapitoly 4;
- osvědčený postup počtu použitých druhů PAI při hodnocení se změnil z minimálních 3 na minimálních 6;
- požadavky FIDO na hodnocení detekce biometrického prezentačního útoku byly přesunuty do kapitoly 7;

- odstranění přílohy A: Role v testování PAD v mobilních zařízeních;
- další změny formulací menšího rozsahu za účelem sladění s ISO/IEC 30107-3.

Seznam všech částí souboru ISO/IEC 30107 lze nalézt na webových stránkách ISO a IEC.

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

Úvod

Prezentace artefaktu nebo lidských charakteristik do subsystému biometrického zachycení způsobem určeným k interferenci s politikou systému se označuje jako prezentační útok. Soubor ISO/IEC 30107 se zabývá technikami pro automatickou detekci prezentačních útoků. Tyto techniky se nazývají mechanismy detekce prezentačního útoku (PAD). ISO/IEC 30107-3 stanovuje principy a metody pro posouzení výkonnosti mechanismů PAD a pro podávání zpráv o jejich výsledcích.

Mechanismy PAD jsou běžně integrovány do mobilních zařízení používajících biometriku^{[1][2]}. Následující vlastnosti mobilních zařízení vyžadují vývoj profilu ISO/IEC 30107-3 specifického pro mobilní zařízení:

- Mobilní zařízení mají často zrychlené časové osy vývoje produktů, takže čas a zdroje pro testování PAD mohou být omezené.
- Jeden typ biometrického subsystému je často integrován do široké škály mobilních zařízení, takže výsledky jednoho testu mohou být použitelné pro více typů mobilních zařízení se stejným operačním systémem (OS) nebo používající stejný vývojový jazyk.
- Biometrické subsystémy integrované do mobilních zařízení jsou obvykle uzavřené systémy, takže testování výkonnosti probíhá v rámci hodnocení celého systému.

Tento dokument poskytuje požadavky na posouzení výkonnosti mechanismů PAD v mobilních zařízeních s lokálním biometrickým rozpoznáváním. Obecný profil s požadavky na hodnocení detekce biometrického prezentačního útoku je uveden v kapitole 5, stejně jako profil specifický pro rychlou online identitu (FIDO) uvedený v kapitole 6^[3].

1 Předmět normy

Tento dokument představuje profil, který specifikuje požadavky na testování mechanismů detekce biometrického prezentačního útoku (PAD) v mobilních zařízeních s lokálním biometrickým rozpoznáváním a v biometrických modulech integrovaných do mobilních zařízení.

V profilu jsou uvedeny požadavky z ISO/IEC 30107-3, které jsou specifické pro mobilní zařízení. Rovněž stanovuje požadavky, které nejsou obsaženy v ISO/IEC 30107-3. Pro každý požadavek profil stanovuje „Přístup k testování PAD pro mobilní zařízení“. U některých požadavků jsou číselné hodnoty nebo rozsahy uvedeny jako osvědčené postupy.

Tento profil je použitelný pro mobilní zařízení, která fungují jako uzavřené systémy bez přístupu k interním výsledkům, včetně mobilních zařízení s lokálním biometrickým rozpoznáváním a také biometrických modulů pro mobilní zařízení.

Tento dokument se nevztahuje na mobilní zařízení s výhradně vzdáleným biometrickým rozpoznáváním.

K útokům uvedeným v tomto dokumentu dochází na zařízení pro zachycení během prezentace a sběru biometrických charakteristik. Jakékoli další útoky jsou mimo rozsah tohoto dokumentu.

Konec náhledu - text dále pokračuje v placené verzi ČSN.