ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Květen 2025**

Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

ČSN ISO/IEC 30107-1

36 9862

Information technology – Biometric presentation attack detection – Part 1: Framework

Technologies de l,information – Détection d,attaque de présentation en biométrie – Partie 1: Structure

Tato norma je českou verzí mezinárodní normy ISO/IEC 30107-1:2023. 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 30107-1:2023. 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 2382-37 zavedena v ČSN EN ISO/IEC 2382-37 (36 9001) Informační technologie – Slovník – Část 37: Biometrika

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).

Vysvětlivky k textu převzaté normy

Pro účely této normy byly použity následující anglické termíny v původní podobě, vzhledem k rozšíření těchto termínů v odborné komunitě a/nebo absenci českého ekvivalentu:

front end, back end.

Vypracování normy

Zpracovatel odborného překladu: Ing. Vladimír Pračke, IČO 40654419

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.

MEZINÁRODNÍ NORMA

Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

ISO/IEC 30107-1
Druhé vydání
2023-08

ICS 35.240.15

Obsah

Strana

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 směrnicích 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 směrnicích 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. 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 JTC1 *Informační technologie*, subkomise SC 37 *Biometrika*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 30107-1:2016), které bylo technicky zrevidováno.

Hlavní změny jsou:

– termíny a definice byly harmonizovány s ostatními částmi souboru ISO/IEC 30107.

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

Biometrické technologie se používají k rozpoznávání jednotlivých osob na základě biologických a behaviorálních charakteristik. Proto jsou často používány jako součást bezpečnostních systémů. Bezpečnostní systém podporovaný biometrickou technologií se může pokusit rozpoznat osoby, které jsou známy jako přátelské nebo nepřátelské, nebo se může pokusit rozpoznat osoby, které takto nejsou systému známy.

Od počátku těchto technologií se všeobecně uznává možnost podvržení rozpoznání odhodlanými protivníky stejně jako potřeba protiopatření k detekci a zmaření podvržených pokusů o rozpoznání nebo prezentačních útoků. K narušení zamýšlené funkce biometrické technologie může dojít v kterémkoli místě bezpečnostního systému a jakýmkoli subjektem, ať už jde o osobu zevnitř organizace nebo vnějšího protivníka. Soubor ISO/IEC 30107 má však omezený rozsah a zaměřuje se na mechanismy pro automatizovanou detekci prezentačních útoků prováděných subjekty biometrického zachycení na zařízení pro zachycení během prezentace biometrických charakteristik. Tyto automatizované mechanismy se označují jako metody „detekce prezentačního útoku“ (PAD). Morfingové útoky, kdy jsou během registrace předkládány biometrické vzorky, které jsou manipulovány tak, aby se shodovaly se dvěma nebo s více subjekty biometrických dat, nejsou v souboru ISO/IEC 30107 brány v úvahu, ačkoli metody hodnocení výkonnosti jsou pro mechanismy detekce PAD a morfingových útoků podobné.

Možnost podvracení biometrických systémů v místě sběru dat odhodlanými jednotlivci jednajícími jako subjekty biometrického zachycení omezila použití biometriky v aplikacích, které nejsou pod dohledem agenta vlastníka systému, jako jsou vzdálené sběry dat prostřednictvím nedůvěryhodných sítí. Například směrnice pro elektronickou autentizaci z tohoto důvodu nedoporučují používat biometriku jako autentizační faktor. U bezobslužných aplikací, jako je vzdálená autentizace přes otevřené sítě, lze ke zmírnění rizik útoku použít automatizované metody detekce prezentačních útoků. Normy, nejlepší postupy a nezávisle hodnocené mechanismy mohou zlepšit bezpečnost všech systémů využívajících biometriku, ať už používají zachycení dat s dohledem či bez dohledu, včetně těch, které používají biometrické rozpoznávání k zabezpečení online transakcí.

Stejně jako v případě biometrického rozpoznávání jsou mechanismy PAD zatíženy chybami, a to jak falešně
pozitivními, tak falešně negativními: falešně pozitivní indikace nesprávně kategorizují bona-fide prezentace jako útoky, čímž zhoršují účinnost systému, a falešně negativní indikace nesprávně kategorizují prezentační útoky jako bona-fide prezentace, aniž by zabránily narušení bezpečnosti. Proto rozhodnutí použít konkrétní implementaci PAD závisí na požadavcích aplikace a zvážení kompromisů s ohledem na bezpečnost a účinnost.

Účelem tohoto dokumentu je poskytnout základ pro PAD definováním pojmů a ustavením rámce, jehož prostřednictvím lze specifikovat a detekovat události prezentačních útoků, aby mohly být kategorizovány, podrobně popsány a komunikovány pro následné rozhodovací činnosti a posuzování výkonnosti biometrického systému. Tento základ bude také přínosem pro další normalizační projekty v komisích a subkomisích ISO/IEC. Tento
dokument neobhajuje konkrétní mechanismus jako standardní nástroj PAD.

V současné době má soubor ISO/IEC 30107 další tři části. ISO/IEC 30107-2 definuje datové formáty pro předávání typu přístupu používaného při detekci biometrických prezentačních útoků a pro předávání výsledků metod PAD. Datové formáty definované v ISO/IEC 30107-2 jsou integrovány do rozšiřitelných formátů pro výměnu biometrických dat definovaných v souboru ISO/IEC 39794. ISO/IEC 30107-3 ustanovuje principy a metody pro posuzování

výkonnosti mechanismů PAD. ISO/IEC 30107-4 poskytuje požadavky na posuzování výkonnosti mechanismů PAD na mobilních zařízeních s lokálním biometrickým rozpoznáváním.

1 Předmět normy

Tento dokument ustanovuje termíny a definice, které jsou užitečné při specifikaci, charakterizaci a hodnocení metod detekce prezentačního útoku (PAD).

Tento dokument neposkytuje následující informace:

- standardizaci konkrétních PAD metod detekce;
- podrobné informace o protiopatřeních (tj. mechanismech proti falšování), algoritmech nebo senzorech;
- celkové posouzení bezpečnosti nebo zranitelností na úrovni systému.

Útoky, které jsou v tomto dokumentu zvažovány, jsou útoky, ke kterým dojde na zařízení pro zachycení během prezentace a sběru biometrických charakteristik. Jakékoli jiné útoky jsou považovány za útoky mimo rozsah tohoto dokumentu.