ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Březen 2019**

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 30107-1:2016. 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 30107-1:2016. It was translated by the Czech Agency for Standardization. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 2382-37:2012 nezavedena1)

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:

anti-spoofing

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 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.

MEZINÁRODNÍ NORMA

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

ISO/IEC 30107-1
První vydání
2016-01-15

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. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

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 ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými 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 obdržených ISO (viz www.iso.org/patents).

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

Vysvětlení významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy WTO týkající se technických překážek obchodu (TBT), jsou uvedeny na tomto odkazu URL: Foreword – Supplementary information.

ISO/IEC 30107-1 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 37 *Biometrika*.

ISO/IEC 30107 se společným názvem *Informační technologie – Detekce biometrického prezentačního útoku* se sestává z následujících částí*:*

- *Část 1: Rámec*
- *Část 2: Datové formáty*
- *Část 3: Testování a podávání zpráv*

Úvod

Biometrické technologie jsou používány k rozpoznání jednotlivých osob na základě biologických a behaviorálních charakteristik a následně jsou často používány jako součást bezpečnostních systémů. Biometrická technologie napomáhající bezpečnostnímu systému se může pokusit rozpoznat osoby, které jsou systému známy jako přátelské nebo nepřátelské, nebo se může pokusit rozpoznat osoby, které takto nejsou systému známy.

Od počátku těchto technologií byla možnost narušení rozpoznání odhodlanými protivníky široce uznávána, stejně jako zde byla potřeba s použitím protiopatření detekovat a zmařit podvratné pokusy o rozpoznání nebo prezentační útoky. Narušení zamýšlené funkce biometrické technologie se může odehrávat v jakémkoliv místě v rámci systému bezpečnosti a jakýmkoliv aktérem, ať už je to interní pracovník nebo vnější protivník. Tato mezinárodní norma (ISO/IEC 30107) je co do rozsahu omezená, je však zaměřená na techniky pro automatizovanou detekci prezentačních útoků, provedených subjekty biometrického zachycení v místě prezentace, a shromažďování příslušných biometrických charakteristik. Budeme tuto automatizovanou techniku nazývat metody „Detekce prezentačního útoku“ (Presentation Attack Detection (PAD)).

Možnost narušení biometrických systémů v okamžiku shromažďování dat určenými jedinci, působícími jako subjekty biometrického zachycení, omezuje použití biometriky v aplikacích, nad kterými neprovádí dohled agent vlastníka systému, jako je například vzdálené shromažďování přes nedůvěryhodné sítě. Směrnice o e-autentizaci například nedoporučují z tohoto důvodu použít biometriku jako autentizační faktor. V neobsluhovaných aplikacích, jako je vzdálená autentizace přes otevřené sítě, mohou být metody automatické detekce prezentačního útoku použity na zmírnění rizik útoku. Normy, doporučené postupy a nezávisle hodnocené techniky by mohly zlepšit bezpečnost všech systémů využívajících biometriku, ať už používají zachycení dat pod dohledem nebo bez dohledu, včetně těch, které používají u bezpečných online transakcí biometrické rozpoznávání.

Jak je tomu v případě biometrického rozpoznávání, techniky PAD jsou předmětem chyb, jak falešně pozitivních, tak falešně negativních: falešně pozitivní indikace nesprávně kategorizují obvyklé prezentace jako útoky, a tím narušují efektivitu systému, a falešně negativní indikace nesprávně kategorizují prezentační útoky jako obvyklé, nezabraňující narušení bezpečnosti. Rozhodnutí použít specifickou implementací PAD tedy bude záviset na požadavcích aplikace a zvážení kompromisů s ohledem na bezpečnost a efektivitu.

Záměrem této části ISO/IEC 30107 je poskytnout základ pro PAD definováním termínů a ustavením rámce, prostřednictvím kterého mohou být události prezentačního útoku specifikovány a detekovány, aby mohly být kategorizovány, podrobně popsány a komunikovány pro následné přijímání rozhodnutí o biometrickém systému a činnostech
týkajících se posouzení výkonu. Tento základ bude také prospěšný pro další projekty norem v komisích a subkomisích ISO/IEC. Tato mezinárodní norma nepodporuje specifickou techniku jako standardní nástroj PAD.

Existují dvě další části ISO/IEC 30107. Část 2 definuje datové formáty pro vyjádření typu přístupu použitého při detekci biometrického prezentačního útoku a pro vyjádření výsledků metod detekce prezentačního útoku. Část 3 stanoví principy a metody pro posouzení výkonnosti algoritmů nebo mechanismů detekce prezentačního útoku.

1 Předmět normy

Tato část ISO/IEC 30107 ustavuje termíny a definice, které jsou užitečné při specifikaci, charakterizování a hodnocení metod detekce prezentačního útoku.

Mimo rozsah předmětu normy jsou

- normalizace specifických metod detekce PAD;
- podrobné informace o protiopatřeních (tj. techniky anti-spoofingu), algoritmech nebo senzorech; a
- celkové posouzení bezpečnosti na úrovni systému nebo zranitelnosti.

Útoky zvažované v ISO/IEC 30107 jsou útoky, které probíhají v senzoru v průběhu prezentace a shromažďování biometrických charakteristik.

Jakékoliv další útoky jsou mimo rozsah ISO/IEC 30107.

---

1) ČSN ISO/IEC 2382-37:2014, která přejímala ISO/IEC 2382-37:2012, byla zrušena z důvodu nahrazení mezinárodní normy novějším vydáním z roku 2017. ISO/IEC 2382-37:2017 je zavedena v ČSN ISO/IEC 2382-37:2018.