ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Březen 2019**

Informační technologie –
Detekce biometrického prezentačního útoku –
Část 3: Testování a podávání zpráv

ČSN
ISO/IEC 30107-3

36 9862

Information technology – Biometric presentation attack detection –
Part 3: Testing and reporting

Technologies de l,information – Détection d,attaque de présentation en biométrie –
Partie 3: Essais et rapports dessai

Tato norma je českou verzí mezinárodní normy ISO/IEC 30107-3:2017. 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 30107-3:2017. 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 zavedena v ČSN ISO/IEC 2382-37 (36 9001) Informační technologie – Slovník – Část 37:
Biometrika

ISO/IEC 19795-1:2006 zavedena v ČSN ISO/IEC 19795-1:2008 (36 9861) Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 1: Principy a rámec

ISO/IEC 30107-1:2016 zavedena v ČSN ISO/IEC 30107-1:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

Souvisící ČSN

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

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

ČSN ISO/IEC 15408-3 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro

hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ČSN ISO/IEC 19792 (36 9858) Informační technologie – Bezpečnostní techniky – Hodnocení bezpečnosti biometriky

ČSN ISO/IEC 30107-2 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 2: Datové formáty

Upozornění na národní poznámky

Do normy byly doplněny národní poznámky upozorňující na nesprávné odkazy na dokumenty v Bibliografii.

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, end-to-end, hill-climbing, proxy

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 3: Testování a podávání zpráv

ISO/IEC 30107-3
První vydání
2017-09

ICS 35.240.15

Obsah

Strana

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 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 tomto odkazu URL: www.iso.org/iso/foreword.html.

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

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

Úvod

Na prezentaci artefaktu nebo lidských charakteristik vůči subsystému biometrického zachycení způsobem zamýšlejícím narušit politiku systému je označováno jako prezentační útok. ISO/IEC 30107 (soubor) se zabývá technikami pro automatizovanou detekci prezentačních útoků. Tyto techniky se nazývají mechanismy detekce prezentačního útoku (PAD).

Pokud jde o případ biometrického rozpoznání, mechanismy PAD jsou vystaveny falešně pozitivním a falešně negativním chybám. Falešně pozitivní chyby nesprávně kategorizují bona fide prezentace jako prezentace útoků,
potenciálně označující nebo obtěžující legitimní uživatele. Falešně negativní chyby špatně kategorizují prezentační útoky (známé také jako prezentace útoků) jako bona fide prezentace, potenciálně ústící v prolomení bezpečnosti.

Rozhodnutí použít konkrétní implementaci PAD proto závisí na požadavcích aplikace a zohlednění kompromisů s ohledem na bezpečnost, sílu důkazů a účinnost.

Účelem tohoto dokumentu je:

- definovat termíny souvisící s testováním a podáváním zpráv o detekci biometrického prezentačního útoku, a

- specifikovat principy a metody posouzení výkonnosti detekce biometrického prezentačního útoku, včetně metrik.

Tento dokument je směrován na prodejce nebo testovací laboratoře snažící se provádět hodnocení mechanismů PAD.

Terminologie, praktiky a metodiky testování biometrické výkonnosti pro statistickou analýzu byly normalizovány v rámci ISO a Společných kritérií. Metriky jako FAR, FRR, a FTE jsou široce používány k charakterizování výkonnosti biometrického systému. Terminologie, praktiky a metodiky testování biometrické výkonnosti pro statistickou analýzu jsou pouze částečně použitelné na hodnocení mechanismů PAD v důsledku významných základních rozdílů mezi koncepty testování biometrické výkonnosti a koncepty testování mechanismu PAD. Tyto rozdíly mohou být kategorizovány následovně:

a) Statistická významnost

Testování biometrické výkonnosti využívá statisticky významný počet zástupce testovacích subjektů cílových uživatelských skupin. Neočekává se, že by se chybovosti významně měnily, když se přidá více testovacích subjektů nebo se použije zcela odlišná skupina. Obecně platí, že při více měřeních se zvyšuje přesnost chybovostí.

Při testování PAD může být mnoho biometrických modalit napadeno velkým nebo neurčitým počtem druhů poten-
ciálních nástrojů prezentačního útoku (PAI). V těchto případech je velmi obtížné nebo dokonce nemožné mít komplexní model všech možných nástrojů prezentačních útoků. Mohlo by být proto nemožné nalézt reprezentativní sadu druhů PAI pro hodnocení. Nelze proto předpokládat, že by naměřené chybovosti jedné sady nástrojů prezentačních útoků byly použitelné na odlišnou sadu.

Druhy PAI prezentují zdroj systematické změny v testování. Různé PAI mohou mít významně odlišné chybovosti. Nebo v rámci jakýchkoliv daných druhů PAI bude existovat náhodná varianta napříč

případů série PAI. Počet prezentací požadovaných pro statisticky významné testování bude škálovat lineárně s počtem druhů PAI, které jsou předmětem zájmu. V rámci každého druhu PAI bude nejistota spojená s odhadem chybovosti PAD záviset na počtu testovaných artefaktů a na počtu jednotlivců.

PŘÍKLAD 1 V biometrice otisku prstů je známo mnoho silných materiálů artefaktu, ale jakýkoliv materiál nebo mix materiálů, které mohou prezentovat rysy otisku prstů na biometrický senzor, je možným kandidátem. Protože vlastnosti artefaktu, jako je věk, tloušťka, vlhkost, teplota, míry mixu, a výrobní praktiky mohou mít významný vliv na výstup mechanismu PAD, je snadné definovat desetitisíce druhů PAI používající běžné materiály. Statisíce prezentací by bylo potřebných pro řádnou statistickou analýzu – i tak nemohou být výsledné chybovosti přenášeny na další sadu nových materiálů.

b) Srovnatelnost výsledků testování napříč systémy

Při testování biometrické výkonnosti mohou být chybovosti specifické pro aplikaci, založené na stejném korpusu biometrických vzorků použity k porovnání různých biometrických systémů nebo různých konfigurací. Význam „lepší“ a „horší“ je obecně srozumitelný.

Naproti tomu, když se použijí chybovosti k porovnávání mechanismů PAD, termíny jako „lepší“ mohou značně záviset na zamýšlené aplikaci.

PŘÍKLAD 2 V daném scénáři testování s 10 druhy PAI (prezentovaném 100krát), Systém$_1$ detekuje 90 % prezentací útoků a Systém$_2$ detekuje 85 %. Systém$_1$ detekuje všechny prezentace pro 9 druhů PAI, ale selhává při detekci všech prezentací s 10 druhy PAI. Systém$_2$ detekuje 85 % všech druhů PAI. Co je lepší? V bezpečnostní analýze by byl Systém$_1$ horší než Systém$_2$, protože odhalení 10tého druhu PAI by nasměrovalo útočníka tak, že mohl použít tuto metodu k překažení činnosti zařízení pro zachycení po celou dobu. Jestliže by však útočníkům bylo zabráněno použít 10tý druh PAI, Systém$_1$ by byl lepší než Systém$_2$, protože jednotlivé míry ukazují, že je možné překonat Systém$_2$ všemi druhy PAI.

c) Kooperace

Mnoho testů biometrické výkonnosti se zabývá aplikacemi, jako je například řízení přístupu, ve kterých subjekty spolupracují. Chyby v důsledku nesprávné operace jsou otázkou nedostatku znalostí, zkušeností nebo návodu spíše než úmyslu. Závažné nekooperativní chování v dané skupině není částí základního „biometrického modelu“ a učinilo by stanovené chybovosti téměř nepoužitelné pro testování biometrické výkonnosti.

Testy PAD zahrnují subjekty, jejichž chování není kooperativní. Útočníci se pokusí nalézt a využít jakékoliv slabé místo biometrického systému, obcházením nebo zfalšováním zamýšlené operace. Typy prezentačních útoků, založené na zkušenostech a znalostech testera, mohou dramaticky změnit úspěšnost pro útok. Může být proto obtížné definovat testovací postupy, které měří chybovosti způsobem charakteristickým pro kooperativní chování.

d) Automatizované testování

Při testování biometrické výkonnosti je často možné testovat algoritmy porovnání používající databáze od zařízení nebo senzorů podobné kvality. Výkonnost může být měřena v hodnocení technologie použitím dříve shromážděných korpusů vzorků dle specifikace v ISO/IEC 19795-1.

Při testování PAD mohou být data z biometrického senzoru (například digitalizované obrazy otisku prstů) nedostatečná k provádění hodnocení. Biometrické systémy s mechanismy PAD často obsahují další senzory k detekování konkrétních vlastností a biometrické charakteristiky. Proto databáze předem shromážděná pro konkrétní biometrický systém nebo konfiguraci nemusí být vhodná pro jiný biometrický systém nebo konfiguraci. Dokonce nepatrné změny v hardwaru nebo softwaru mohou učinit dřívější měření nepoužitelná. Obecně je nepraktické ukládat vícevariantní synchronizované signály PAD a opakovaně je přehrát v automatizovaném testování. Automatizované testování není proto často alternativou pro testování a hodnocení mechanismů PAD.

e) Kvalita a výkonnost

Při testování biometrické výkonnosti je výkonnost obvykle spojena přímo s kvalitou biometrických dat. Vzorky nízké kvality obecně vedou k vyšším chybovostem, zatímco test se vzorky pouze vysoké kvality bude mít obecně za následek nižší chybovosti. Z tohoto důvodu jsou metriky kvality často použity ke zlepšení výkonnosti (závislé na aplikaci).

Při testování PAD, i když dokonce i nízká biometrická kvalita může způsobit, že artefakt bude neúspěšný, zde neexistuje žádný důvod předpokládat obecně určitou úroveň kvality z artefaktů. Vzorky z artefaktů mohou projevovat lepší kvalitu než vzorky z lidských biometrických charakteristik. Při absenci modelu dovedností útočníka se zdá opodstatněné (přinejmenším při hodnocení bezpečnosti) předpokládat scénář „nejhoršího případu“, kde útočník vždy použije nejlepší možnou kvalitu. Tak je možné při nejmenším určit zaručenou minimální míru detekce pro konkrétní testovací sadu, při současném snižování počtu nezbytných testů. Je pak věcí ratingu potenciálu útoku úspěšných artefaktů (snaha a odbornost pro potřebnou kvalitu), aby se určila stupeň bezpečnosti, podle obvyklé metody v hodnocení podle Společných kritérií.

Na základě rozdílů a) až e) mohou být odvozeny následující obecné poznámky, týkající se chybovostí a metrik souvisících s mechanismy PAD:

- Při hodnocení jsou druhy PAI analyzovány/ohodnocovány samostatně.

- Chybovosti klasifikace prezentace útoku jiné než 0 % pro druhy PAI pouze ukazují, že PAI může být úspěšný. Odlišný tester může dosáhnout vyšší nebo nižší chybovost klasifikace prezentace

útoku. Kromě toho proškolení v identifikování relevantního materiálu a parametrů prezentace by mohlo zvýšit chybovost klasifikace prezentace útoku pro druhy tohoto PAI. Zkušenosti a odbornost testera, stejně jako dostupnost nutných zdrojů, jsou důležité faktory při testování PAD a jsou vzaty v úvahu při provádění porovnání nebo analýzy výkonnosti.

– Chybovosti pro mechanismy PAD jsou stanoveny konkrétním kontextem daného mechanismu PAD, sady druhů PAI, aplikace, testovacího přístupu a testera. Chybovosti pro mechanismy PAD nejsou nutně srovnatelné s podobnými testy, a chybovosti pro mechanismy PAD nejsou nutně reprodukovatelné různými testovacími laboratořemi.

1 Předmět normy

Tento dokument ustavuje:

- principy a metody pro posouzení výkonnosti mechanismů detekce prezentačního útoku;
- podávání zpráv o výsledcích testování z hodnocení mechanismů detekce prezentačního útoku;
- klasifikace známých typů útoků (v informativní příloze).

Mimo předmět normy jsou:

- normalizace specifických mechanismů PAD;
- detailní informace o opatřeních (tj. anti-spoofing techniky), algoritmech, nebo senzorech;
- celková bezpečnost na úrovni systému nebo posouzení zranitelností.

Útoky zvažované v tomto dokumentu probíhají v senzoru během prezentace. Jakékoli jiné útoky jsou považovány za útoky mimo rozsah tohoto dokumentu.