ČESKÁ TECHNICKÁ NORMA

ICS 35.240.15 **Květen 2024**

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 d,essai

Tato norma je českou verzí mezinárodní normy ISO/IEC 30107-3:2023. 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 30107-3:2023. 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 30107-3 (36 9862) z března 2019.

Národní předmluva

Změny proti předchozí normě

V dokumentu byla doplněna relativní míra přijetí prezentace útoků podvodníka (13.4.4) a byla doplněna příloha C. V textu dokumentu byla provedena upřesnění a zlepšení.

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 15408-1 zavedena v ČSN EN ISO/IEC 15408-1 (36 9789) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ISO/IEC 15408-2 zavedena v ČSN EN ISO/IEC 15408-2 (36 9789) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty

ISO/IEC 15408-3 zavedena v ČSN EN ISO/IEC 15408-3 (36 9789) Informační bezpečnost,

kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

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 dosud nezavedena

Souvisící ČSN

ČSN EN ISO/IEC 18045 (36 9805) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Metodika pro hodnocení bezpečnosti IT

ČSN ISO/IEC 19989 (soubor) (36 9859) Bezpečnost informací – Kritéria a metodika pro hodnocení bezpečnosti biometrických systémů

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

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článcích „Informace
o citovaných dokumentech“ a „Souvisící ČSN“ 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).

Pro účely této normy byl použit následující anglický termín v původní podobě, vzhledem k rozšíření tohoto termínu v odborné komunitě a absenci českého ekvivalentu:

bona fide.

MEZINÁRODNÍ NORMA

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

ISO/IEC 30107-3
Druhé vydání
2023-01

ICS 35.240.15

Obsah

Strana

Předmluva..... 5

Úvod..... 6

1. Předmět normy..... 8

2. Citované dokumenty..... 8

3. Termíny a definice..... 8

3.1. Prvky útoku..... 9

3.2. Metriky..... 10

3.3. Testovací role..... 12

4. Zkratky..... 12

5. Shoda..... 13

6. Přehled detekce prezentačního útoku (PAD)..... 13

7. Stupně hodnocení mechanismů PAD..... 14

7.1..... Přehled..... 14

7.2..... Obecné principy hodnocení mechanismů PAD..... 14

7.3..... Hodnocení subsystému PAD..... 15

7.4..... Hodnocení subsystému zachycení dat..... 15

7.5..... Hodnocení celého systému..... 15

8..... Vlastnosti artefaktu..... 16

8.1..... Vlastnosti PAI v biometrických útocích podvodníka..... 16

8.2..... Vlastnosti PAI v útocích subjektů tajících biometrickou identitu..... 17

8.3..... Vlastnosti syntetizovaných biometrických vzorků s neobvyklými charakteristikami..... 17

9..... Úvahy při nekonformních pokusech zachycení biometrických charakteristik..... 18

9.1..... Metody prezentace..... 18

9.2..... Metody posouzení..... 18

10..... Vytvoření artefaktů a použití v hodnoceních mechanismů PAD..... 18

10.1..... Obecně..... 18

10.2..... Vytváření a příprava artefaktů..... 18

10.3..... Použití artefaktů..... 19

10.4..... Iterativní testování artefaktů s účinnou identitou..... 19

11..... Faktory hodnocení závislé na

procesu..... 20

11.1.....
Přehled..... 20

11.2..... Hodnocení procesu
registrace..... 20

11.3..... Hodnocení procesu
ověřování..... 20

11.4..... Hodnocení procesu
identifikace..... 21

11.5..... Hodnocení off-line mechanismů PAD..... 21

12..... Hodnocení používající rámec Společných kritérií..... 21

12.1..... Obecně..... 21

12.2..... Společná kritéria a biometrika..... 22

12.2.1... Přehled..... 22

12.2.2... Obecné aspekty hodnocení..... 23

12.2.3... Chybovost v testování..... 23

12.2.4... Hodnocení PAD..... 23

12.2.5... Posouzení zranitelnosti..... 24

13..... Metriky pro hodnocení biometrických systémů mechanismy PAD..... 25

13.1..... Obecně..... 25

13.2..... Metriky pro hodnocení subsystému PAD..... 25

13.2.1... Obecně..... 25

13.2.2... Metriky klasifikace..... 26

13.2.3... Metriky neodezvy..... 27

13.2.4... Metriky účinnosti.....

..... 27

13.2.5...

Shrnutí.....
..... 28

13.3..... Metriky pro hodnocení subsystému zachycení dat..... 28

13.3.1...

Obecně.....
..... 28

13.3.2... Metriky získávání.....
..... 28

13.3.3... Metriky neodezvy.....
..... 28

13.3.4... Metriky účinnosti.....
..... 28

13.3.5...

Shrnutí.....
..... 29

13.4..... Metriky pro hodnocení celého systému.....
... 29

13.4.1...

Obecně.....
..... 29

13.4.2... Metriky přesnosti.....
..... 29

13.4.3... Metriky účinnosti.....
..... 29

13.4.4... Zobecněné hodnocení výkonnosti celého systému..... 30

13.4.5...

Shrnutí.....
..... 31

Příloha A (informativní) Klasifikace typů útoků.....
.. 32

Příloha B (informativní) Příklady druhů artefaktů používaných v hodnocení subsystému PAD pro zařízení zachycení otisku prstu.....
..... 35

Příloha C (informativní) Role v testování PAD..... 36

Bibliografie..... 37

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).

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) nebo v seznamu patentových prohlášení obdržených IEC (viz https://patents.iec.ch).

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 30107-3:2017), které bylo technicky zrevidováno.

Hlavní změny jsou:

- byla doplněna relativní míra přijetí prezentace útoku podvodníka (13.4.4);
- byly doplněny informace o rolích při testování detekce prezentačních útoků (příloha C);
- byla provedena obecná technická upřesnění a zlepšení.

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 adrese www.iso.org/members.html a www.iec.ch/national-committees.

Úvod

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

Pokud jde o případ biometrického rozpoznávání, 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 nesprávně 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 biometrické PAD, a
- specifikovat principy a metody posuzování výkonnosti biometrické PAD, včetně metrik.

Tento dokument je směrován na dodavatele 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. Míra chybného přijetí (FAR), míra chybného odmítnutí (FRR), a míra neúspěšné registrace (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 mechanismu testování PAD. Tyto rozdíly mohou být kategorizovány takto:

a) Statistická významnost

Testování biometrické výkonnosti využívá statisticky významný počet subjektů testu, reprezentujících cílovou sku-
pinu uživatelů. Neočekává se, že by se chybovosti významně měnily, když se přidá více subjektů testu nebo se použije zcela odlišná skupina.

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

PAIS prezentují zdroj systematické změny v testování. Různé PAI mohou mít významně odlišné chybovosti. Navíc v rámci jakýchkoliv daných PAIS bude existovat náhodná změna napříč případy série PAI. Počet prezentací požadovaných pro statisticky významné testování bude škálovat lineárně s počtem PAIS, které jsou předmětem zájmu. V rámci každého PAIS 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, avšak jakýkoliv materiál nebo mix materiálů, které mohou prezentovat rysy otisku prstu na biometrické zařízení pro zachycení, je možným kandidátem. Jelikož vlastnosti artefaktu, jako je věk, tloušťka, vlhkost, teplota, poměry smíchání, a výrobní praktiky mohou mít významný vliv na výstup mechanismu PAD, je snadné definovat desetitisíce PAIS používající běžné materiály. Pro řádnou statistickou analýzu by bylo potřebných statisíce prezentací, i tak nemohou být výsledné chybovosti přenášeny na další sadu nových materiálů.

Prezentace PAI může být také zdrojem změn v testu. Změny tlaku, polohy nebo dokonce charakteristiky PAI prezentujícího mohou ovlivnit výkonnost PAD.

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. Výsledky lze použít k jednoznačnému porovnání a posouzení výkonnosti systému. Naproti tomu při použití chybovosti k porovnání mechanismů PAD může být interpretace výsledků vysoce závislá na zamýšlené aplikaci.

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

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 manipulováním 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 ze zařízení nebo senzorů podobné kvality. Výkonnost může být měřena v hodnocení technologie použitím dříve shromážděných korpusů vzorků, jak je uvedeno v ISO/IEC 19795-1.

Při testování PAD mohou být data z biometrického zařízení pro zachycení (například digitalizované obrazy otisku prstu) v některých případech nedostatečná k provádění hodnocení. Biometrické systémy s mechanismy PAD často obsahují přídavné senzory k detekování specifických vlastností biometrické charakteristiky. Proto dříve shromážděná databáze 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 více variantní synchronizované signály PAD a opakovaně je přehrát v automatizovaném testování. Automatizované testování není proto často alternativou pro testování a ohodnocení 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 nízká biometrická kvalita může dokonce 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. Bez 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 specifickou testovací sadu, při současném snižování počtu nezbytných testů. Je pak věcí posouzení potenciálu útoku úspěšných artefaktů (snaha a odbornost pro potřebnou kvalitu), aby se určila úroveň 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 PAIS analyzovány/ohodnocovány samostatně.

– Chybovosti klasifikace prezentace útoku jiné než 0 % pro PAIS pouze ukazují, že PAI může být úspěšný. Odlišný tester může dosáhnout vyšší nebo nižší chybovosti klasifikace prezentace útoku. Kromě toho proškolení v identifikování relevantního materiálu a parametrů prezentace může zvýšit chybovost klasifikace prezentace útoku pro tento PAIS. Zkušenosti a odbornost testera, stejně jako dostupnost nezbytných 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 (PAD);
- podávání zpráv o výsledcích testování z hodnocení mechanismů PAD; a
- klasifikace známých typů útoků (příloha A).

Předmětem normy nejsou:

- normalizace specifických mechanismů PAD;
- detailní informace o protiopatřeních (tj. techniky proti podvrhům), algoritmech, nebo senzorech; a
- celková bezpečnost na úrovni systému nebo posouzení zranitelnosti.

Útoky zvažované v tomto dokumentu probíhají v zařízení pro zachycení během prezentace. Jakékoli jiné útoky jsou považovány za útoky mimo předmět tohoto dokumentu.