ČTRNÁCT NEDOROZUMĚNÍ
OHLEDNĚ BIOMETRICKÉ IDENTIFIKACE A AUTENTIZACE

Červen 2020

www.aepd.es/es
www.edps.europa.eu

Identifikace je postup k identifikaci jednotlivce v rámci skupiny. Tento postup porovnává data jednotlivce, aby byl identifikován ve vztahu k údajům každého jednotlivce v rámci této skupiny. Autentizace je postup prokázání identity tvrzené jednotlivcem. Tento postup porovnává pouze údaje tohoto jednotlivce s údaji tvrzené identity.

Zvýšené užívání biometrických údajů (např. otisků prstů nebo rozpoznávání obličeje pro účely identifikace a autentizace v současnosti vzbuzuje zájem veřejnosti, který je doprovázen určitými nedorozuměními. Tento dokument uvádí a vysvětluje 14 z nich a poskytuje další odborné odkazy za účelem objasnění.

1. „Biometrická informace je uchovávána v samotném algoritmu.“

Algoritmus je metoda, přednastavená sada operací nebo návod, nikoli však prostředek pro uchovávání biometrických údajů.

Shromážděné biometrické informace (např. obrázek otisku prstu) jsou zpracovávány dle standardně definovaných postupů[1] a výsledek tohoto postupu je uložen v datových záznamech, tzv. podpisech, vzorcích nebo šablonách. Tyto vzorce číselně zaznamenávají fyzické vlastnosti, čímž umožňují rozlišit jednotlivé osoby.

Nicméně, existují techniky strojového učení, které předávají části svých tréninkových datových sad modelům, které vytvářejí.[2] Některé z těchto technik jsou užívané při biometrické identifikaci a autentifikaci.

---

[1] Viz datový formát otisku prstů ISO 19794-2: https://www.ekds.gov.tr/bio/FM3_README.pdf (page 2); pro podrobnější příklad vlastnoručního podpisu viz: R.Pizarro Santos, Análisis de las normas internacionales de firmas manuscritas ISO/ IEC 19794-7 y 19794-11, Universidad de Carlos III, Madrid 2010,: https://e-archivo.uc3m.es/bitstream/handle/10016/10990/PFC_Rob-erto_Pizarro_Santos.pdf?sequence=1&isAllowed=y

[2] Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. 2017. Machine Learning Models that Remember Too Much. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 587–601. DOI: https://doi.org/10.1145/3133956.3134077

2. *„Užívání biometrických údajů je stejně rušivé jako jakýkoliv jiný identifikační/autentizační systém.“*

Na rozdíl od hesla nebo certifikátu, shromážděné biometrické údaje odhalují o subjektu v průběhu procesu autentifikace nebo identifikace více informací. V závislosti na shromážděných biometrických údajích mohou být o subjektu dovozeny takové údaje jako rasa nebo pohlaví (dokonce z otisku prstů[3]), duševní stav, nemoci, genetické vlastnosti, fyzické vady, užívání látek atd.[4] Protože je tato informace „vestavěná“, uživatel nemůže zabránit shromažďování těchto dalších informací.

3. *„Biometrická identifikace/autentizace je přesná."*

Na rozdíl od postupů založených na heslu nebo certifikátech, které jsou 100 % přesné (např. heslo se shoduje nebo neshoduje), biometrická identifikace/autentizace je založena na pravděpodobnosti (např. sejmutý otisk prstu je z 96 % podobný jednomu z X). Existuje určitá míra chybné shody (přijetí neoprávněné osoby) a chybné neshody (odmítnutí oprávněné osoby). Tyto poměry jsou tím vyšší, čím nepřesnější je snímací zařízení, a také záleží na podmínkách, za kterých se sejmutí uskutečnilo (například světlo v místnosti nebo čistota senzoru).[5] Přesnost některých biometrických údajů, jako jsou například otisky prstů, závisí na věku osoby a je ovlivněná jejím stárnutím.[6]

4. *„Biometrická identifikace/autentizace je natolik přesná, aby vždy rozlišila mezi dvěma osobami.“*

Je prokázáno, že biometrická podobnost mezi sourozenci nebo příbuznými je pro biometrické systémy matoucí.[7] Předmětem studia je především identita biometrických vzorů pro identifikaci dvojčat nad rámec rozpoznávání obličeje.[8] Navíc podmínky v nekontrolovaných prostředích

---

[3] Více informací o údajích, které mohou být získány z otisku prstů: The Hidden Data in Your Fingerprints. Scientific American (27/04/2018) https://www.scientificamerican.com/article/the-hidden-data-in-your-fingerprints

[4] Sekundární (soft) biometrika zkoumá nejedinečné vlastnosti jednotlivce na základě jeho biometrické informace, jako je duševní stav, zdraví atd. Fairhurst, Michael; Li, Cheng; Da Costa-Abreu, Márjory: 'Predictive biometrics: a review and analysis of predicting personal characteristics from biometric data', IET Biometrics, 2017, 6, (6), p. 369-378, DOI: 10.1049/iet-bmt.2016.0169 IET Digital Library, https://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2016.0169

[5] Více informací o nedostatcích britského policejního systému pro rozpoznávání obličeje v: UK police use of facial recognition technology a failure, says report. The Guardian (15/05/2018) https://www.theguardian.com/uk-news/2018/may/15/uk-police-useof-facial-recognition-technology-failure

[6] Galbally, Javier & Haraksim, Rudolf & Beslay, Laurent. (2018). A Study of Age and Ageing in Fingerprint Biometrics. IEEE Transactions on Information Forensics and Security. PP. 1-1. 10.1109/TIFS.2018.2878160. https://www.researchgate.net/publication/328526153_A_Study_of_Age_and_Ageing_in_Fingerprint_Biometrics

[7] Viz příklad, jak uživatelé mohou oklamat Iphone technologii pro rozpoznávání obličeje: The iPhone X's Face ID thinks these two brothers are the same person. MSPoweruser (5/11/2017) https://mspoweruser.com/iphone-xs-face-id-thinks-two-brothers-person

[8] K. W. Bowyer and P. J. Flynn, "Biometric identification of identical twins: A survey," 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), Niagara Falls, NY, 2016, pp. 1-8, doi: 10.1109/BTAS.2016.7791176. https://www3.nd.edu/~kwb/Bowyer_Flynn_BTAS_2016.pdf

(rozpoznávání obličeje na veřejném prostranství nebo užívání obličejových nebo antivirových masek) vedou ke zvýšené chybovosti, a tudíž je záměna pravděpodobnější.

5. *„Biometrická identifikace/autentizace je vhodná pro všechny osoby.“*

Někteří lidé nemohou užívat určitý typ biometriky, protože jejich fyzické vlastnosti systém nerozpozná. V případě zranění, nehod, zdravotního stavu (jako je ochrnutí) a dalších, může být tato nekompatibilita dočasná. Trvalá biometrická nekompatibilita může být jedním z faktorů vedoucích ke společenskému vyloučení.[9]

6. *„Postup biometrické identifikace/autentifikace nelze obejít.“*

Existují postupy a techniky, které umožňují obejít biometrické autentizační systémy a předstírat identitu jiné osoby. Některé z těchto postupů a technik, jako je používání masek[10] nebo kopírování otisků prstů,[11] nevyžadují rozsáhlé technické znalosti nebo ekonomické zdroje. Tzv. „nepřátelské systémy“ jsou speciálně navrženy k přelstění obrazových rozpoznávacích systému a mohou být užity k přelstění biometrické identifikace.[12]

7. *„Biometrická informace nemůže být prozrazena.“*

Na rozdíl od postupů založených na heslu nebo certifikátu, většina osobních biometrických vlastností není chráněna a může být zachycena na dálku (například obličej, otisky prstů, směr pohybu, tepelné otisky obvykle nejsou skryty.

Na druhé straně, ti jednotlivci, kteří chtějí aktivně předcházet biometrickému sledování nebo obelstít identifikační systémy, k tomu budou mít příslušné nástroje,[13] zatímco velká většina populace je nebude využívat.

---

[9] Více informací o rizicích sociálního vyloučení u britského biometrického systému průkazů totožnosti: UK Identity Cards and Social Exclusion. Privacy International (May 2005)https://privacyinternational.org/sites/default/files/2017-12/UK%20Identity%20Cards.pdf

[10] Hackeři prolomili FaceID u IphoneX za použití 3D masky. Wired UK (13/11/2017) https://www.wired.co.uk/article/hackers-trick-apple-iphone-x-face-id-3d-mask-securit

[11] Budete k tomu přilepeni. Studenti z Mumbai college oklamali biometrický systém. Hindustan Times (15/05/2017) https://www.hindustantimes.com/mumbai-news/you-will-be-glued-to-this-mumbai-college-s-students-trick-biometric-system/story-W64f1jdMtecxKDml2DakeI.html

[12] Pautov, Mikhail et al. “On Adversarial Patches: Real-World Attack on ArcFace-100 Face Recognition System.” 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON) (2019): n. pag. Crossref. Web. https://arxiv.org/pdf/1910.07067.pdf

[13] Tyto oděvy používají výstřední prvky k oklamání softwaru pro rozpoznávání obličeje, aby software nepoznal, že se jedná o člověka. V Business Insider (5/6/2020) https://www.businessinsider.com/clothes-accessories-that-outsmart-facial-recognition-tech-2019-10?IR=T#images-fromechizens-lab-shows-how-the-visor-blocks-ais-ability-to-detect-a-face-6

Pokud nebudou přijata žádná opatření ke snížení rizika nebo neoprávněného použití biometrických údajů, jejich použití bude stejné, jako bychom měli naše přístupové heslo napsané na čele.[14]

8. „Jakékoliv biometrické zpracování předpokládá identifikaci/autentizaci."

Nikoliv nezbytně. Například zpracování biometrických údajů pohybu myši využívané k určení toho, zda k webové stránce přistupuje robot, využívá zacházení s biometrickou informací pro účely rozlišení člověka od stroje. Zpracování biometrických údajů může být dále prováděno ke zjištění, zda se lidský nebo zvířecí narušitel pohybuje v určitém prostoru nebo k v případě digitálních systémů rozlišujících muže, žen a dětí.[15] Stále však existuje riziko zpracování takových informací k jinému než původnímu účelu, např. v případě bezpečnostního selhání, regulační změny nebo nezákonného zpracování.

9. „Biometrické identifikační/autentizační systémy jsou pro uživatele bezpečnější."

V každém z mnoha systémů, ve kterých jsou zpracovávány naše biometrické údaje, může dojít k porušení zabezpečení. Neoprávněný přístup k biometrickým údajům v systému by umožnil nebo ulehčil (v případě více autentizačních faktorů) přístup k dalším systémům užívajícím tytéž biometrické údaje. Mohlo by to mít stejný následek jako v případě používání stejného hesla u různých odlišných systémů, tudíž rozsah použití biometriky je sám o sobě problém. Navíc, na rozdíl od systémů založených na heslu, jednou kompromitovaná biometrická informace nemůže být změněna nebo zrušena.

Pokud byla dříve biometrická informace uložena v několika databázích (hlavně pro účely veřejné bezpečnosti nebo kontroly na hranicích), nyní je ukládána ve zvyšujícím, se počtu zařízení. To velmi zvyšuje pravděpodobnost porušení bezpečnosti únikem biometrických údajů (během jejich shromažďování, přenosu, uložení nebo jiného zpracování), k čemuž již dochází.[16]

10. „Biometrická autentizace je silná."

Dle definice je silný autentizační systém takový, který vyžaduje poskytnutí alespoň dvou faktorů z toho, co znáte, máte nebo jste (biometrika). Dle definice je autentizační proces používající pouze biometrické údaje slabý, zatímco použití přístupové karty a hesla je silné. Biometrická autentizace často vyžaduje předchozí registraci nebo identifikaci, u které je,

---

[14] Vědci získávají otisky prstů z fotografií pořízených ze vzdálenosti až tří metrů. Bleeping Computer (12/01/2017) https:// www.bleepingcomputer.com/news/security/scientists-extract-fingerprints-from-photos-taken-from-up-to-three-meters-away/

[15] Španělská CaixaBank nabízí schůzku k sejmutí obličeje (facial recognition): https://www.caixabank.es/particular/banca-digital/face-id_en.html

[16] Příklad porušení bezpečnosti odhalující miliony biometrických údajů: nový únik dat odhaluje miliony záznamů otisků prstů a sejmutých obličejů (facial recognition) (14/08/2019) https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breachhas-exposed-millions-of-fingerprint-and-facial-recognition-records-report

například u rozpoznávání obličeje, nutné porovnání s fotografií v dokladu totožnosti. Pokud je ale po identifikačním postupu autentizační proces pouze biometrický, je systém slabý.

11. „Biometrická identifikace/autentizace je uživatelsky přívětivější."

Záleží na použité technologii, okolnostech, vnímání a kultuře každého uživatele. Kromě popsaného problému vhodnosti u páté nedorozumění (viz výše), zde mohou být další problémy, které negativně ovlivní vnímaní uživatele: pocit narušení soukromí, selhání biometrických systémů, které zabrání přístupu ke službám, neexistence nebo nevhodnost nebiometrických alternativ nebo potřeba provést registraci u každé entity.[17]

12. „Biometrickou informaci převedenou do hashe nelze obnovit."

Ke zvýšení bezpečnosti zpracování biometrických informací je doporučeno odstranit biometrický vzor, ze kterého byl získán *hash*[18] nebo *biohash*[19]. Nicméně existují studie, které ukazují, že *hash* může být „návratný", tzn. že je možné získat původní biometrický vzor, a to zvláště v případě, když je porušeno tajemství klíče užitého ke generování *hash(e)*.[20]

13. „Uložená biometrická informace neumožňuje rekonstrukci původní biometrické informace, ze které byla získána."

Uložená biometrická informace (tj. vzor) umožňuje částečnou rekonstrukci původního biometrického údaje (např. obličej). Taková částečná rekonstrukce biometrického údaje má často dostatečnou přesnost pro to, aby ji jiný biometrický systém rozpoznal jako původní údaj. Existují např. studie obličejové biometrické informace, které ukazují, že je možné získat věrohodné zobrazení z robotického portrétu (počítačem vytvořený portrét).[21] Přesnost rekonstrukce závisí na množství shromážděných biometrických informací.

---

[17] Španělská CaixaBank nabízí schůzku k sejmutí obličeje (facial recognition). https://www.caixabank.es/particular/banca-digital/face-id_en.html

[18] Hashovací funkce je postup, který přemění jakoukoliv datovou sadu (například vzorec otisku prstů) na řetězec (znakovou řadu) s pevnou délkou, a to nezávisle na velikosti vstupních dat. Více informací o hashovací funkci a jejím využití jako pseudonymizační techniky na: https://edps.europa.eu/data-protection/our-work/publications/papers/introduction-hash-function-personal-data_en

[19] Biohashing je technika, při které dochází ke kombinaci náhodného čísla a biometrických údajů. Více informací na: https://www.researchgate.net/publication/234809846_Remarks_on_BioHash_and_its_mathematical_foundation

[20] Více informací o biohash(ovacích) inverzních útocích: Topcu, B., Karabat, C., Azadmanesh, M. et al. Practical security and privacy attacks against biometric hashing using sparse recovery. EURASIP J. Adv. Signal Process. 2016, 100 (2016) https://link.springer.com/article/10.1186/s13634-016-0396-1#Sec5. Více informací o tom, jak může být získán vzorec z biohash(e) na: Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar. Handbook of Fingerprint Recognition. Springer Science & Business Media (2009) https://books.google.es/books?id=1Wpx25D8qOwC&pg=PA407&lpg=PA407&dq=BIOHASHING&source=bl&ots=9yS_1Spp9&sig=ACfU3U3VkdF7ybO2p8jfhOhslMnAEhL8A&hl=es&sa=X&ved=2ahUKEwiUqMfNpPznAhWLxYUKHSkiDmk4ChDoATAFegQIChAB#v=onepage&q=BIOHASHING&f=false

[21] Srovnání původních obličejů a obličejů rekonstruovaných ze vzorců na straně 3: Michelle Chibba and Alex Stoianov. On Uniqueness of Facial Recognition Templates. Information and Privacy

14. „Biometrická informace není interoperabilní.“

Naopak, systémy zpracovávající biometrické informace jsou vyvíjeny podle takových standardů, aby se zajistila jejich interoperabilita.[22] Systémy, které porovnávají výsledek *hashovací* funkce aplikované na biometrické vzory, mohou být interoperabilní jednoduchou metodou, a to sdílením klíčů použitých při *hashovacím* procesu.

Neoficiální překlad článku pořídil Úřad pro ochranu osobních údajů České republiky.

Commissioner's Office of Ontario, Canada March 2014 https://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf

[22] Příklady přeměn biometrických formátů v: Convert fingerprints to ISO and ANSI fingerprint template data format https://jomutech.com/convertfingerprintimagestoisooransifingerprinttemplateformats Popis biometrických interoperabilních standardů naleznete na: http://biometria611.blogspot.com/p/estandares.html