

Biometrika a její rizika

Biometrika v kontextu informačních technologií představuje metody automatizovaného rozpoznávání a ověřování identity osob na základě jejich unikátních fyzických nebo behaviorálních (chování) charakteristik. Slouží k zodpovězení otázek „Kdo jste?“ (identifikace) nebo „Jste skutečně tím, za koho se vydáváte?“ (autentizace). V rámci vícefázového ověřování plní roli faktoru inherence („něco, co jsem“).

Základní typy biometrie

Fyziologická biometrie: Zkoumá statické fyzické rysy lidského těla. Mezi nejběžnější patří skenování otisků prstů, rozpoznávání obličeje (např. Face ID), skenování sítnice nebo duhovky oka, analýza geometrie ruky či rozložení žil v dlani. Řadí se sem i analýza DNA, ta se však nepoužívá pro běžný přístup k IT systémům.

Behaviorální biometrie: Zaměřuje se na dynamické vzorce chování, které se člověk učí a které si osvojil. Jde například o dynamiku stisku kláves (rytmus a rychlost psaní na klávesnici), analýzu pohybu a gestikulace myši, styl chůze (zachycený gyroskopy a akcelerometry v telefonu) nebo hlasovou biometrii (způsob mluvy, frekvence, tón).

Hlavní rizika a zranitelnosti

Neodvolatelnost (Neměnnost) biometrických dat: Toto je nejkritičtější slabina biometrie. Pokud dojde k úniku textového hesla nebo PINu, uživatel si jej jednoduše změní. Pokud ale hackeři z databáze odcizí digitální mapu otisků prstů nebo obličejů, uživatel tyto své fyzické rysy nemůže nikdy změnit. Kompromitovaná biometrie je kompromitována natrvalo a může být zneužívána po zbytek života oběti.

Spoofing a Presentation Attacks (Prezentační útoky): Útočník se snaží oklamat senzor podvrženými biometrickými daty. V závislosti na kvalitě senzoru to může zahrnovat použití silikonových odlitků otisků prstů, fotografií ve vysokém rozlišení zobrazených na displeji tabletu pro oklamání kamery, případně sofistikované 3D masky.

Deepfakes a AI útoky: S masivním nástupem generativní umělé inteligence čelí zejména hlasová biometrie a systémy pro rozpoznávání tváří novému typu hrozeb. Útočníkovi dnes stačí krátký zvukový záznam oběti k syntetizaci jakékoliv věty, což umožňuje obcházet systémy hlasového ověřování u bank nebo při Vishingových útocích.

Chybovost systémů (FAR a FRR): Žádný biometrický systém nefunguje se stoprocentní přesností. Existují dvě základní metriky chybovosti, které jdou často proti sobě. FAR (False Acceptance Rate) označuje riziko, že systém nesprávně vpustí neoprávněnou osobu (např. velmi podobného sourozence). FRR (False Rejection Rate) znamená, že systém naopak odmítne oprávněného uživatele (např. kvůli špinavému prstu, zranění, změně osvětlení nebo nošení brýlí).

Ochrana soukromí a hromadné sledování: Biometrická data patří k nejcitlivějším osobním údajům (GDPR je přímo klasifikuje jako zvláštní kategorii osobních údajů). Pokud jsou data centralizována,

hrozí jejich zneužití k plošnému sledování obyvatelstva, profilování nebo k identifikaci osob na veřejných prostranstvích pomocí kamerových systémů bez jejich souhlasu.

Ochrana a bezpečné nasazení

Lokální zpracování (On-device autentizace): Nejlepší prevencí proti úniku biometrických databází je jejich nevytváření. Moderní standardy pro běžné uživatele (FIDO, Apple Face ID, Windows Hello) fungují tak, že biometrický vzor nikdy neopouští dané zařízení. Je bezpečně uložen v šifrovaném hardwarovém čipu (Secure Enclave nebo TPM čip). Senzor pouze lokálně porovná tvář/prst se vzorem a do sítě odešle pouze kryptografický certifikát, že ověření proběhlo úspěšně.

Liveness Detection (Detekce živosti): K obraně proti prezentačním útokům (fotografie, masky, odlitky) musí senzory aktivně testovat, zda interagují s živou tkání. Využívá se měření teploty, průtoku krve v kapilárách, sledování mikropohybů a mrkání očí, nebo nasazení 3D hloubkových infračervených senzorů namísto běžných 2D kamer.

Fallback mechanismy a vícefázový přístup: Biometrie by nikdy neměla být jediným bodem selhání. Vždy musí existovat záložní způsob ověření (Fallback), například bezpečný PIN pro případ zranění prstu nebo poruchy senzoru. V nejkritičtějších infrastrukturách se biometrie používá zásadně jako druhý faktor ve spojení s něčím, co uživatel má (např. čipová karta), nikoliv samostatně.

From:

<http://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

<http://serviceit.cz/doku.php?id=it:sec:biometrics>

Last update: **2026/06/06 14:59**

