Máme se bát biometrie?

Neustálou inovací dnešní moderní společnosti se stává biometrika (věda zabývající se jedinečnými prvky člověka) stále častějším pojmem pro vývoj všech odvětví.

Do oblasti zabezpečovacích technologií tak vnáší zcela nový rozměr. Například IT společnosti se předhánějí o co nejvíce sofistikované zabezpečení přístupu k důvěrným datům uživatele. Integrací čtečky otisku prstů se předhánějí všichni přední výrobci a nutno uznat – daří se jim to!

Kromě odvětví zabezpečovacích technologií je zjevné využití biometriky ve zbrojním průmyslu, který, jak už to bývá, je často průkopníkem významných inovací. V současné době se zbrojní průmysl zaměřuje například na vývoj biometrických snímačů umístěných na „chytrých" zbraních (smart guns), které brání zneužití zbraně v případě jejího odcizení. V neposlední řadě nutno zmínit i v dnešních dnech tak nejistý automobilový průmysl, který se pochopitelně také nedrží stranou od zabezpečení biometrickou technologií.

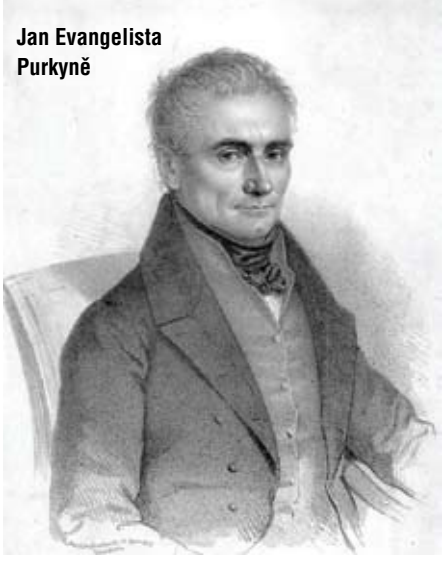
Zatímco před pár lety byla biometrika neprozkoumanou oblastí a čtečka otisku prstů patřila do oblasti výjimečných produktů, v dnešní době je integrace čtečky otisků prstů do zabezpečovacích systémů nabízena všemi předními společnostmi a stává se do jisté míry standardem.

Biometrice se zkrátka v posledních pár letech daří úspěšně se rozvíjet. V závislosti na vývoji se na trh dostávají biometrické snímače různých vlastností a technologií pro ověření osobních biologických charakteristik. Z nejpraktičtějších jsou to otisky prstů, snímek obličeje nebo oční sítnice. V posledních letech se začínají objevovat dokonce snímače ověřující krevní řečiště, otisk pod povrchem kůže nebo DNA snímané osoby.

Kdo položil stavební kámen pro biometrii?

Za průkopníka biometriky, jak ji známe dnes, je vědeckou společností stále považován český přírodovědec Jan Evangelista Purkyně (1787 – 1869). Ten v roce 1823 vydal ve Vratislavi 54stránkové dílo, v němž popsal základní vzory papilárních linií na koncových článcích prstů a klasifikoval je do 9 vzorů. V pozdějších letech bylo matematickými metodami vypočteno, že existují 64 miliardy různých variant v uspořádání papilárních linií, přičemž se vycházelo pouze z obrazce jednoho prstu. Odhadnutý vzrůst počtu obyvatelstva zeměkoule je maximálně na 16 miliard. Pokud se tato teorie rozšíří na všech deset prstů, výsledné číslo je následně vyjádřeno desátou mocninou 64 miliard. Tím byla prakticky vyloučena možnost výskytu dvou jedinců se stejným obrazcem papilárních linií.

Přesto v posledních letech v kriminalistice stoupá procento záměn při identifikaci osob podle otisků prstů. Odhad četnosti těchto záměn je 0,8 %. Vyvozuje se tak, že jen v USA je ročně chybně identifikováno 1900 otisků prstů. Jako nejznámější chyba bývá uváděn případ právníka Brandona Mayfielda, který byl „omylem" obviněn ze spáchání teroristického útoku.



Jan Evangelista Purkyně

Důvěra široké veřejnosti v biometriku je potom pod vlivem takovýchto pochybení, a také vinou stále malé znalosti biometrie, značně narušena. Nepochopení principů biometriky pak může vést například k bláhové představě, že ke zneužití např. otisku prstu stačí, aby ho někdo nositeli uřízl. Spousta lidí si také myslí, že se v případě poranění prstu nedostanou do střeženého prostoru. Jiní si otisky ze zcela nepochopitelných důvodů cíleně poškozují, jelikož jim jejich zaměstnavatel pořídil biometrický terminál docházky. Naivní je také představa, že je možné získat kopii otisku přímo z terminálu.

Co nás tedy vede ke strachu ze sdílení otisku prstu? Jsou-li tyto technologie tak nespolehlivé, jak se říká, a proč by se tedy světové vlády usnesly na využití biometriky v cestovních dokladech, kdyby ji bylo možné tak jednoduše zneužít? Co nám může biometrika přinést, a co vzít?

Jak biometrie vůbec funguje?

Využití biometriky v zabezpečovacích systémech přináší vysokou míru jistoty a bezpečnosti. Spokojenost uživatelů ale vždy závisí na správném pochopení jejich požadavků a jejich zohlednění v systému. Základními parametry, které je třeba zvážit, je cílová skupina, která systém bude užívat, a v neposlední řadě volba správné technologie čtení. V dnešní době se na trhu pohybuje několik typů snímačů, jako jsou například: optoelektronické, kapacitní, teplotní, elektroluminiscenční, radiofrekvenční, a nově také možnost multispektrální analýzy otisku. Všechny tyto technologie poskytují poměrně širokou škálu možností, přičemž každý má své výhody a nevýhody, které je třeba zvážit.

Nejpoužívanější snímače v dnešní době jsou optoelektronické, které umožňují jednoduché sejmutí otisku CCD detektorem, využívající osvětlení celé plochy prstu. Odrážené světlo pak prochází luminoforní vrstvou k CCD detektoru, kde se vytvoří

obraz otisku. Výhodami této nejrozšířenější a nepoužívanější technologie je vysoká kvalita čtení, statická odolnost a rezistence vůči vlivům okolního prostředí. Na druhou stranu je třeba si dát pozor na některé nevýhody. Například znečištění nebo poškození prstu může způsobit jeho nekorektní vykreslení na otisku. Stejně tak otisk zůstávající na detektoru může zkreslit další pořizované otisky.

Další rozšířenou technologií jsou kapacitní snímače, které využívají rozdílu kapacitního odporu mezi deskou snímače a povrchem prstu. Papilární linie jsou k podložce přilehlejší než mezery mezi nimi, mají tedy vyšší odpor. Poměrně jednoduchý princip přitom zajišťuje vysokou kvalitu čtení. Snímače také příjemně překvapí malým rozměrem a nízkou cenou. Bohužel doba jejich životnosti je relativně malá, vlivem statické elektřiny se postupně ničí a je nutné je v rozmezí přibližně tří let měnit. I když finančně tato okolnost může být nevýznamná, přece jen znamená potíže z organizačního hlediska.

Zmínit lze také teplotní snímače, které pořizují otisk prstu snímáním rozdílných teplot, které mají papilární linie a mezery mezi nimi. Uživatel při snímání přejíždí prstem přes citlivou plochu, obraz se skládá do digitálních pásů a poté do výsledného otisku. U této metody existuje nebezpečí, že při několikanásobném přejíždění prstem přes snímač bude sejmuta vždy jiná část prstu, což výrazně limituje možnost vytvoření databáze otisků. Navíc tyto snímače neposkytují dostatečně vysokou kvalitu obrazu otisku, a proto nejsou pro použití v přístupových systémech vhodné.

V posledních měsících byly na trh společnostmi uvedeny multibiometrické terminály, s nimiž lze uživatele identifikovat i pomocí tváře. Tyto terminály samozřejmě umožňují i snímání otisku prstu, a zvyšují tak bezpečnost chráněné oblasti. Kamera snímající tvář pracuje na principu infračervené kamery s vysokým rozlišením, a je tedy nemožné ji obejít například fiktivní fotografií uživatele.

Absolutní špičkou mezi snímači otisků prstů je Americká firma Lumidigm. Systém využívající více osvětlovacích soustav o rozdílných vlnových délkách tak dokáže prosvítit otisk prstu a porovnat i s otiskem pod povrchem kůže, krevní řečiště a teplotu prstu. Snímač je tak maximálně rezistentní proti falzifikátům otisku jako třeba silikonový prst. Tato technologie umožňuje čtení při extrémních podmínkách. Navíc vyhodnocovací software dokáže dotvořit

Detail multispektrální analýzy

otisk v případě neúplného přitisknutí prstu na snímač. Díky multispektrální analýze lze jasně detekovat v místě přitlačení i slabý odtok krve z prstu, a jasně tak oddělit falsifikát od skutečného prstu.

Volba správného systému?

Pro posouzení kvality biometrických snímačů existuje několik základních parametrů. Prvním a bezesporu nejdůležitějším je přesnost, se kterou dokáže snímač odlišit autorizovanou osobu od neautorizované. Z hlediska přesnosti se zjišťují dva parametry – pravděpodobnost chybného zamítnutí, jež se dá vyjádřit následující větou: otisk je shodný s otiskem v databázi, ale je zamítnut, bývá vyjadřováno zkratkou FRR – False Reject Rate, a pravděpodobnost chybné akceptace, která má následující definici: otisk nesouhlasí s otiskem v databázi, ale je přijat, která je vyjadřována zkratkou FAR – False Accept Rate.

Pravděpodobnost chybného zamítnutí tedy udává procento, kdy biometrický identifikační systém zamítne autorizovanou osobu jako neidentifikovatelnou nebo neověřenou. Přestože je tato chyba z hlediska bezpečnosti méně významná než FAR, ve skutečnosti způsobuje zdržení, nespokojenost a frustraci uživatelů. Na druhou stranu pravděpodobnost chybné akceptace udává procento událostí, kdy neautorizovaná osoba je identifikačním systémem přijata jako autorizovaná.

Mezi ukazateli FRR a FAR existuje nepřímá úměra. Čím je systém striktnější, FAR klesá, naopak tak roste pravděpodobnost zamítnutí osoby, která má oprávnění ke vstupu. Naopak u „benevolentnějších" systémů je FRR nízká, ale nebezpečí autorizace neoprávněnou osobou je vyšší. Obě hodnoty tedy závisí na požadavcích uživatele, zvoleném systému a rozdílu/rozdílech v technologiích.

Je možné dostat fotografii otisku ze snímače?

Získat fotografii či jakkoli vykonstruovat otisk prstu uložený v databázi je prakticky nemožné. Biometrické systémy pracují s matematickými výpočty otisku papilár, kdy jsou z každého otisku vybrány specifické body, a ty následně zakódovány do databáze. Kdyby se následně útočník snažil prolomit databázi, objevil by pouze nesystematickou soustavu čísel určujících body na prstech, nikoliv však konkrétní otisk, který by bylo možné jakkoli zobrazit v plné podobě.

Svěřit bezpečnost biometrii?

Dnešní doba biometriku posunula opravdu kupředu, není to jen zajímavá část vědecko-fantastických filmů. Také díky vývoji předních výrobců se biometrické systémy staly i cenově dostupným doplňkem většiny přístupových systémů. Z praxe je známo, že vhodnou analýzou cílového prostředí a výběrem vhodného biometrického snímače je docíleno velmi vysokého stupně zabezpečení a ušetření nákladů jak při nákupu identifikátorů, tak i například kvalitním výstupem z docházkových systémů. Identifikátory, jak je známo, může uživatel kdykoliv ztratit, půjčit či jakkoli zneužít.

Vezměte si s sebou váš vlastní nezaměnitelný klíč, otisk máte vždy při ruce. ■

Tomáš Karásek
produktový manažer EZS a EKV
ABBAS, a. s.
Edisonova 5, Brno
tel.: +420 541 240 956
e-mail: tomas.karasek@abbas.cz
www.abbas.cz

Příklad použití falzifikátu otisku prstu

Foto: archiv firmy LUMIDIGM a autora