IDENTIFIKÁCIA POUŽÍVATEĽA PRI PRÁCI S MOBILNÝM ZARIADENÍM NA ZÁKLADE BIOMETRICKÝCH CHARAKTERISTÍK

Identification of Users During Usage of Mobile Devices Based on Behavioral Biometrics

Michal Slovík

MOTIVÁCIA

V mobilných zariadeniach ľudia vykonávajú rôzne činnosti ako správu e-mailov, prezeranie webových stránok, ale aj prácu s rôznymi typmi dát (fotografie, hudba, video). K všetkým týmto dátam a činnostiam je častokrát nutné spojenie so vzdialeným serverom alebo aplikáciou, ktorá vykonáva komunikáciu namiesto nás.

Prihlásenie sa do týchto systémov (alebo aj do samotného mobilného zariadenia) je ťažkopádne, ak si chceme prečítať iba jeden e-mail alebo odoslať fotografiu na sociálnu sieť. Na druhej strane, používatelia si volia jednoduché vzory alebo heslá a preto existujú možnosti, ako toto zabezpečenie obísť [1]. Zvolenie jednoduchých hesiel má negatívny dopad na bezpečnosť mobilných zariadení, preto je výhodné použiť systém na rozpoznávanie používateľa na základe biometrických charakteristík, pretože môže zjednodušiť pristupovanie k mobilným zariadeniam.

Nielen prihlasovanie môže byť problém, ale aj určitá zmena prostredia, ktorú systémy na rozpoznávanie používateľa zvyknú zanedbávať môže byť problematická. Ako najjednoduchší príklad je zmena prstu, ktorým používateľ píše alebo ťahá po obrazovke mobilného zariadenia. Ďalším príkladom je dynamická zmena pohybu, napríklad chôdza, vstávanie a pod. Pri týchto činnostiach dochádza ku zmenám, ktoré je potrebné brať do úvahy.

1 ÚVOD DO PROBLEMATIKY

Systémy na modelovanie používateľa na základe biometrických charakteristík môžu mať rôzne ciele, ktoré sa snažia dosiahnuť: Identifikácia a autentifikácia, autentifikácia, rozpoznávanie emócií, expertízy, a pod. Identifikácia je proces, v ktorom systém zisťuje identitu osoby na základe jej biometrických charakteristík a porovnáva ich so šablónou. To znamená zachytenie biometrických charakteristík aktuálneho používateľa a následné porovnanie so vzorom a prípadne akceptovanie alebo zamietnutie na základe určenej hranice [2].

Ďalej rozlišujeme rôzne druhy biometrických charakteristík, ktoré sú využívané pri autentifikácií alebo identifikácií. Rozdeľujeme ich na dve základne kategórie: fyziologické a behaviorálne. Fyziologické sa zameriavajú na statické prvky ako napríklad odtlačok prsta, geometria ruky, črty tváre, zrenica oka. Behaviorálne sú určené na základe vzťahu k správaniu používateľa. používateľa počas rôznych činnosti, ako rozprávanie, písanie na klávesnici, alebo aj pri chôdzi. Pri mobilných zariadeniach (smartfónoch) napríklad môžeme sledovať tieto charakteristiky a z nich odvodiť numerické hodnoty, napríklad dĺžku stlačenia klávesy alebo objektu, veľkosť stlačenej plochy, rýchlosť pohybu prsta po obrazovke, silu stlačenia klávesy alebo objektu.

Vo všeobecnosti môžeme popísať modelovanie používateľa pre jeho identifikáciu obrázkom:

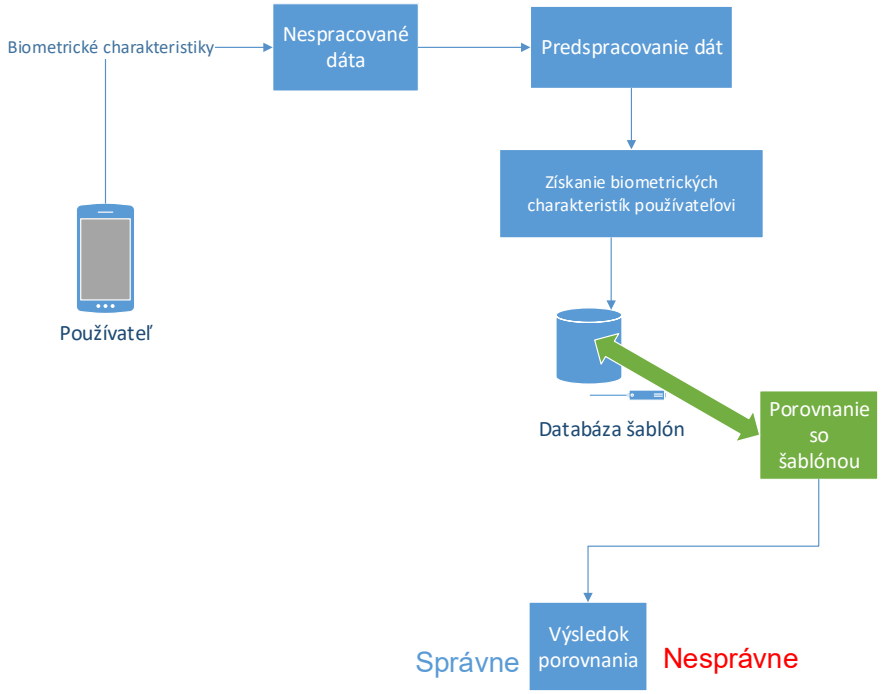

Figure 1: Modelovanie používateľa pomocou biometrických charakteristík

Proces spracovania biometrických charakteristík pozostáva z dvoch hlavných fáz, zápis (angl. enrollment) a rozpoznávanie (angl. recognition). Počas fázy zápisu sa surové dáta získavajú od používateľa a sú ukladané v databáze spolu s identitou používateľa. Získané dáta sú predspracované a rozdelené podľa zvolených kritérií, napríklad podľa ukončenia gesta, alebo podľa

určitého času (1s). Málo výrazné charakteristiky sa môžu zahodiť, napríklad charakteristiky, ktoré sú podobné pre všetkých používateľov. Počas fázy rozpoznávania sa biometrické charakteristiky znovu získavajú od individuálneho používateľa a porovnávané s uloženými dátami pre stanovenie identity používateľa.

Pre stanovenie identity používateľa môžeme použiť viaceré možnosti. Jednou z možností sú vzdialenostné metriky(angl. distance metrics) ako napríklad Euklidová vzdialenosť, Hammingova vzdialenosť a mnohé iné. Ďalšou možnosťou je použitie metódy strojového učenia (machine learning algorithms, supervised learning algorithms) [3]. V systémoch zabezpečených heslom je nutné, aby medzi dvoma reťazcami nastala presná zhoda pre overenie používateľa, pri biometrických charakteristikách sa rozhoduje o totožnosti osoby na základe tejto vzdialenosti. Ideálne biometrické charakteristiky musia mať malú množinu významných čŕt špecifických pre používateľa (inter-user variations) [2]. Zároveň tieto množiny charakteristík by sa nemali prelínať s ostatnými používateľmi, pretože systém by mohol nájsť zhodu s nesprávnym používateľom. V praxi sa tieto podmienky nemôžu úplne splniť vzhľadom na nedostatok informácii (nedostatok jedinečnosti) v šablóne.

Keďže sa rozhodujeme na základe vzdialenostných metrík, pri rozpoznávaní používateľa nezískame 100% úspešnosť, a aby sme dokázali vyhodnotiť úspešnosť metód rozpoznávania na základe biometrických charakteristík používame miery EER (Equal error rate), FAR (False acceptance rate), FRR (False rejection rate) a mnohé ďalšie metriky na vyhodnotenie presnosti biometrických systémov. Ako prvé si vysvetlíme EER. Ide o hodnotu, ktorá udáva že podiel chybných prijatí sa rovná podielu falošných odmietnutí. To znamená, čím nižšie je EER hodnota, tým vyššia je presnosť biometrického systému). Spolu s touto hodnotou sa vyhodnocujú aj pravdepodobnosti FAR a FRR. Pravdepodobnosť chybného prijatia (FAR) je miera pravdepodobnosti, že systém na základe biometrických charakteristík nesprávne príjme neoprávnenému používateľovi. Miera falošného odmietnutia (FRR) je miera pravdepodobnosti, že systém na základe biometrických charakteristík nesprávne odmietne pokus o prístup oprávneného používateľa. Obe tieto hodnoty (FAR a FRR) sme schopní nastaviť podľa určitej prahovej hodnoty a tak regulovať jednotlivé pravdepodobnosti. Keď sa tieto hodnoty (FAR a FRR) prelínajú hovoríme o EER. Systémy využívajúce biometrické charakteristiky na mobilných zariadeniach boli spočiatku založené na stlačení a dĺžke držania určitej klávesy [4]. Neskôr sa ukázalo, že kombinácia viacerých biometrických charakteristík (verifikácia tváre, hlasu a podpisu) môže znižovať EER.

Avšak aj samotný používateľ môže zasiahnuť a zmeniť nečakane svoje charakteristické črty a tým ovplyvniť výsledok identifikácie. Príkladom môže byť výmena rúk, v ktorej používateľ drží mobil, ktorý zachytáva biometrické charakteristiky a pri tejto výmene rúk nedokáže rozpoznať túto zmenu a znova vyhodnotí biometrické charakteristiky pre iného používateľa [5]. Podobný problém opisujú Blanco-Gonzalo a spol. [6], kde na základe kresleného vzoru zisťovali stres používateľa. A snažili sa eliminovať rozdiel vo veku, kedy sa môže s narastajúcim vekom zvyšovať trasenie rúk. Zanedbávali však výber prsta, ktorým používateľ daný text písal [6].

S prostredím sa dá pracovať rôzne. V ďalšom prípade sa D. Cazzato a spol [7] venujú získavania biometrických charakteristík z tváre človeka. Ako najväčší problém s prostredím vnímali osvetlenie a natočenie tváre. Čo sa týka problému s natočením tváre alebo celej hlavy iným smerom, vedeli na základe rozpoznania šošovky oka celkom presne zistiť odchýlku tváre od zapamätaného vzoru, a tak počítať s touto zmenou. Rôzne typy osvetlenia, napríklad bežné vonkajšie osvetlenie, osvetlenie celej tváre lampou alebo osvetlenie iba určitej časti tváre, tvorili tri základne typy osvetlení, v ktorom skúšali rozpoznávať používateľa a porovnať výsledky. V konečnom dôsledku iba vypočítali priemer z týchto troch meraní pri odlišnom osvetlení a vznikol im model pre všeobecne osvetlenú tvár.

Ďalšou možnosťou ako sa vysporiadať s problémov prostredia môže byť zachytávanie väčšie množstva charakteristík ako v prípade Drosou a spol [8] kde zaznamenávali pohyb ramien, lakťa, prstov a oddelene od toho prsty. Potom tieto charakteristiky predspracovali a na základe Dynamic Time Warping [8] klasifikátora rozhodovali o autentifikácii používateľa. Podobne riešenie uvádzajú Derawi, Gafurov, a spol [9], kde spájajú dve rozdielne charakteristiky. Behaviorálnu charakteristiku chôdzu a fyziologickú charakteristiku, odlačok prsta.

2 ZÁMER

V tejto práci sa chceme zamerať na identifikáciu a autentifikáciu používateľa na základe biometrických charakteristík, ktoré zaznamenáme pomocou mobilného zariadenia. Rozpoznávanie používateľa by malo byť možné aj v meniacich sa podmienkach, napríklad výmena rúk alebo prsta.

Na základe analýzy sme sformulovali tieto hypotézy: Domnievame sa, že zmena polohy tela (vstávanie zo stoličky, chôdza) ovplyvňuje identifikáciu a autentifikáciu používateľa do značnej miery, ale zároveň nezabraňujú správnemu určeniu identity používateľa. Ďalej sa domnievame, že výmena rúk(ľavej namiesto pravej, alebo naopak) je možné zapracovať do identifikácie a autentifikácie používateľa. Používateľ bude rozpoznaný bez ohľadu na to akú ruku použil.

Tieto hypotézy by sme sa snažili dokázať. Zamerať by sme sa chcel na identifikáciu a autentifikáciu používateľov na základe získaných dát, ktoré by sme pred-spracovali a rozdelili podľa určitého kritéria. Takto pred-spracované dáta pridelili k jednému používateľovi. Týmto spôsobom by sme získali šablónu jeho charakteristických čŕt. Týmto spôsobom získame biometrické charakteristiky od viacerých používateľov. Následne ich rozdelíme na trénovacie a testovacie. Trénovacie biometrické charakteristiky budú slúžiť ako vzor pre konkrétneho používateľa. Testovacími biometrickými charakteristikami bude testovať náš systém, či dokáže rozpoznať správneho používateľa, teda používateľa, ktorému tieto charakteristiky patria. Po tomto rozdelení a vyhodnotení úspešnosti rozpoznania používateľa, sa budeme snažiť skúmať, ako podmienky (zmena polohy tela, výmena rúk) vplývajú na presnosť identifikácie používateľa. Získaný rozdiel potom použiť pri ďalšej identifikácii a autentifikácií.

SKRATKY

EER Equal error rate

FAR False acceptance rate

FRR False rejection rate

LITERATÚRA

[1] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, jan 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6331527/

[2] A. K. Jain, A. A. Ross, and K. Nandakumar, *Introduction to Biometrics*. Boston, MA: Springer US, 2011. [Online]. Available: http://link.springer.com/10.1007/978-0-387-77326-1

[3] S. Z. Li and A. Jain, Eds., *Encyclopedia of Biometrics*. Boston, MA: Springer US, 2009. [Online]. Available: http://link.springer.com/10.1007/978-0-387-73003-5

[4] F. Alshanketi, I. Traore, and A. A. Ahmed, "Improving Performance and Usability in Mobile Keystroke Dynamic Biometric Authentication," in *2016 IEEE Security and Privacy Workshops (SPW)*. IEEE, may 2016, pp. 66–73. [Online]. Available: http://ieeexplore.ieee.org/document/7527755/

[5] A. L. Fantana, S. Ramachandran, C. H. Schunck, and M. Talamo, "Movement based biometric authentication with smartphones," in *2015 International Carnahan Conference on Security Technology (ICCST)*. IEEE, sep 2015, pp. 235–239. [Online]. Available: http://ieeexplore.ieee.org/document/7389688/

[6] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and E. Bella-Pulgarin, "Automatic usability and stress analysis in mobile biometrics," *Image and Vision Computing*, vol. 32, no. 12, pp. 1173–1180, 2014.

[7] D. Cazzato, A. Evangelista, M. Leo, P. Carcagnì, and C. Distante, "A low-cost and calibration-free gaze estimator for soft biometrics: An explorative study," 2016.

[8] A. Drosou, D. Ioannidis, D. Tzovaras, K. Moustakas, and M. Petrou, "Activity related authentication using prehension biometrics," *Pattern Recognition*, vol. 48, no. 5, pp. 1743–1759, May 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031320314004968

[9] M. O. Derawi, D. Gafurov, R. Larsen, C. Busch, and P. Bours, "Fusion of gait and fingerprint for user authentication on mobile devices," in *2010 2nd International Workshop on Security and Communication Networks (IWSCN)*, May 2010, pp. 1–6.