NASK PRACUJE NAD SYSTEMEM UWIERZYTELNIANIA BIOMETRYCZNEGO WYKORZYSTUJĄCEGO SMARTFONY

Niezależny od producentów smartfonów system, który bez użycia wyspecjalizowanych czujników rozpozna użytkownika na podstawie np. obrazu twarzy, linii papilarnych, kształtu dłoni czy próbki głosu, może w niedalekiej przyszłości wejść do użycia. Prace nad nim zaczęły się niedawno w Państwowym Instytucie Badawczym NASK.

NASK jest liderem projektu BioMobi - systemu zdalnego biometrycznego uwierzytelniania na niespecjalizowanych urządzeniach mobilnych, np. na smartfonach. Podstawowym elementem wyróżniającym system jest stosowanie powszechnie dostępnych urządzeń, bez specjalizowanych sensorów biometrycznych. Drugim wyróżnikiem jest to, że rozwiązania będzie można adaptować do sytuacji, co pozwoli na wykorzystanie różnych modalności biometrycznych zależnie od potrzeb bezpieczeństwa i preferencji użytkownika. Projekt, finansowany ze środków Narodowego Centrum Badań i Rozwoju, w którym udział bierze też Politechnika Łódzka i Akademia Górniczo-Hutnicza, zakończy się w 2021 roku.

„Idea była taka, żeby stworzyć system biometryczny, który jest uniezależniony od producentów konkretnych czujników biometrycznych, bo ci producenci mają zamknięte rozwiązania – mówi koordynator projektu prof. Andrzej Pacut, kierownik Zakładu Biometrii i Inteligencji Maszynowej w NASK. - Można jednak wyobrazić sobie system multibiometryczny, czyli taki, który ma możliwość pomiaru wielu modalności biometrycznych i - wykorzystując niespecjalizowane czujniki - daje podobne rezultaty, co system zamknięty”.

Podobne systemy są oferowane przez zaledwie kilka firm na świecie. Co więcej, ocena ich wiarygodności jest utrudniona, gdyż firmy chronią się przed testowaniem swoich metod.

Biometria dostępna dla wszystkich

Podstawowym założeniem projektu jest wykorzystanie standardowych smartfonów, obecnych powszechnie na rynku. Nie chodzi tutaj jedynie o wyspecjalizowane urządzenia wyposażone we wbudowane sensory, odczytujące np. linie papilarne. Dzięki temu poprawi się jakość i wygoda rozpoznawania zdalnego, taki sposób uwierzytelniania ulegnie rozpowszechnieniu, a to wszystko przełoży się na podniesienie poziomu cyberbezpieczeństwa.

Specjaliści z NASK zamierzają stworzyć system wykorzystujący kamery, mikrofony, głośniki, a może nawet czujniki do badania równowagi w smartfonach. Do identyfikacji użytkownika posłużą obraz i dźwięk. ”Jeśli chodzi o obrazy, to zajmujemy się przede wszystkim obrazem twarzy, tęczówką, odciskiem palca, kształtem dłoni i liniami dłoni, być może dołączymy podpis odręczny, w sensie dynamiki podpisu, a nie obrazka podpisu. Jeśli chodzi o dźwięk, to oczywiście głównie chodzi o

rozpoznawanie na podstawie mowy” – wylicza koordynator. Większość z tych modalności wymaga specyficznych metod przystosowanych do zastosowań mobilnych.

Bezpieczeństwo bez dozoru

Jedną z kwestii, z którą muszą zmierzyć się uczestnicy projektu, jest zapewnienie prawdziwości wprowadzanych danych, gdyż system będzie działał na urządzeniach mobilnych, czyli bez dozoru. „Jeśli ktoś nie jest obserwowany, to może np. zamiast twarzy pokazać kartkę papieru, zamiast odcisku palca posłużyć się udającą linie papilarne nakładką na palec. Przy czujnikach dobrej jakości jest to do wykrycia, ale tutaj będzie to trudniejsze” – zaznacza koordynator projektu. Dlatego naukowcy muszą wybrać metody biometryczne, które spełnią wymogi bezpieczeństwa i znaleźć najlepsze sposoby zapobiegania fałszerstwom. Jest to zagadnienie praktycznie nie w pełni jeszcze rozwiązane.

Z założenia wybór poszczególnych modalności będzie zależny od poziomu bezpieczeństwa, jakiego zażyczy sobie użytkownik. Im większa potrzeba zabezpieczeń, tym bardziej skomplikowane muszą być obliczenia. Użytkownik urządzenia dodatkowo będzie miał możliwość zaakceptowania modalności.

Dane biometryczne – bezpieczeństwo przechowywania

Kolejne zagadnienie, które stoi przed specjalistami z NASK, to stworzenie pełnego biometrycznego systemu rozpoznawania, a więc np. podjęcie zasadniczych decyzji dotyczących miejsca i sposobu przechowywania danych biometrycznych, a także miejsca przetwarzania danych na wzorce biometryczne. Jednym z rozwiązań może być przesyłanie danych do specjalnej jednostki, określanej jako „zaufana trzecia strona”, która by je przechowywała i przetwarzała. Rozwiązanie to jest oczywiście niebezpieczne ze względu na konieczność przesyłania danych biometrycznych i niebezpieczeństwo ich przechwycenia. W tej chwili panuje przekonanie, że najlepiej trzymać wszystkie dane biometryczne w telefonie, ale z kolei moce obliczeniowe mogą nie być wystarczające. Możliwe są również rozwiązania hybrydowe. Ponadto, przed przesłaniem danych można je w pewien sposób zniekształcić, aby nie zostały wykorzystane przez niepowołane osoby.

Prof. Pacut przyznaje, że trudność będzie się wiązała również z bazami danych, gdyż nie ma jeszcze wytycznych jasno specyfikujących rozumienie przepisów o danych osobowych RODO dla biometrii. Sytuacji nie ułatwia również fakt, że ludzie niechętnie udostępniają swoje dane biometryczne, a bez tego nie da się przeprowadzić pewnych badań.

Kolejne etapy projektu

Pierwsze zadanie w projekcie, polegające na rozważeniu struktury całego systemu, zostało już ukończone. Następnym zadaniem będzie – w ramach projektu technicznego - stworzenie dla poszczególnych technik biometrycznych algorytmów rozpoznawania tych cech i zabezpieczanie prawdziwości wprowadzanych danych, po to, aby zaimplementować je w postaci programów, które będą tworzone później. W następnych etapach ma powstać wersja produkcyjna.

Rozważane jest testowe wdrożenie systemu na jednej z uczelni wyższych, by studenci mogli dostawać się do określonych zasobów przez zabezpieczenia biometryczne.

Projekt „System zdalnego mobilnego uwierzytelniania biometrycznego wykorzystujący niespecjalizowane urządzenia mobilne (BioMobi)”, którego dofinansowanie wyniosło z II Konkursu CyberSecIdent 7 126 788 zł, zakończy się 31 sierpnia 2021 r.

Źródło: NASK