

BIOMETRIA

dla konsumentów

Elektroniczny DNA ułatwia dostęp do pojazdów i zwiększa bezpieczeństwo

Antoinette Price

Odcisk palców, dłoń, tęczęwka, głos, rozpoznawanie twarzy i gestu pomogą w rozwoju systemów wspomagania kierowcy i bezpieczeństwa pojazdów.

Biometria jest stosowana od dziesięcioleci przez organy ścigania oraz w systemach służących identyfikowaniu osób i kontrolowaniu dostępu, które wymagają wysokiego poziomu zabezpieczeń. Systemy te porównują dane behawioralne i fizyczne.

Niedawno ten zasięg rozszerzył się. Już teraz możemy zabezpieczyć dostęp do smartfonów lub tabletów odciskiem palca lub używać aplikacji rozpoznawania głosu do uwierzytelniania internetowych kont bankowych.

Działać z normami

Komitety techniczne IEC i ich podkomitety tworzą Normy Międzynarodowe w celu zapewnienia niezawodności, jakości i interoperacyjności.

Wspólny Komitet Techniczny ISO/IEC JTC 1 zajmuje się technologiami informacyjnymi. Zakres ISO/IEC JTC 1/SC 37 *Biometrics* obejmuje specyfikacje dotyczące bezpieczeństwa, testowania i raportowania różnych aspektów, takich jak format wymiany danych, rozpoznawanie twarzy, rozpoznawanie komend głosowych.

Odcisk palca - klucz do Twojego samochodu

W miarę jak samochody stają się bardziej połączone i zmiernają do pełnej samodzielności, przemysł motoryzacyjny również zmierza w tym kierunku. Raport Frost i Sullivan mówi, że do roku 2025 jeden na trzy samochody (prawie 34 miliony samochodów osobowych) będzie używać biometrii do identyfikacji i personalizacji.

Zabezpieczenia dla pojazdów

W 2016 r. rekordowa liczba firm technologicznych współpracowała z producentami samochodów, które coraz częściej włączają inteligentne funkcje do swoich najnowszych pojazdów. W badaniach przeprowadzonych przez firmę Gartner szacuje się, że do 2020 r. po drogach będzie poruszać się ćwierć miliarda samochodów połączonych. Jednak jednym z największych wyzwań będzie zabezpieczenie ogromnej liczby danych, które takie samochody tworzą, i ochrona pasażerów przed ich zhakowaniem.

Wiele nowych samochodów ma systemy wykorzystujące biometrię - są one albo wbudowane, albo prowadzone przez zewnętrzne usługi, takie jak chmura.

W przyszłości zwiększy się liczba funkcji, które będą zawierać dodatkowe zabezpieczenia:

- Uruchamianie i obsługa przyszłych samochodów będzie wymagała identyfikacji kierowcy za pomocą czujnika linii papilarnych, będącego uzupełnieniem klucza.
- Inne systemy będą rozpoznawać twarz kierowcy przed wejściem do pojazdu; włączenie silnika będzie możliwe tylko wtedy, gdy będzie aktywny profil kierowcy.
- Rozpoznawanie tęczy zostanie użyte do odblokowania zapłonu, identyfikowania użytkowników pojazdu i spersonalizowanych ustawień (np. foteli czy lusterek).

Bezpieczeństwo kierowcy na nowym poziomie

Sektory: samochodowy, ubezpieczeniowy i zdrowotny będą współdziałać, ponieważ zaawansowana biometria sprawi, że przyszłe samochody będą bardziej bezpieczne. Mimo że miną jeszcze lata zanim samochody będą jeździć autonomicznie, a ludzie nie będą musieli nimi kierować, przemysł motoryzacyjny już opracowuje sposoby monitorowania czujności kierowcy. Na przykład czujniki w pasach i osłonach będą monitorować uderzenia rytmu serca kierowcy i ostrzegać przed zawałem, podczas gdy sensory śledzące oczy wykryją senność prowadzącego pojazd. Praca IEC/TC 47 *Semiconductor devices* obejmuje projektowanie, produkcję i użytkowanie czujników.

Pojawienie się innowacyjnych urządzeń do zarządzania zdrowiem w połączeniu ze starzeniem się populacji, zwiększenie świadomości zdrowotnej i rosnąca potrzeba zarządzania chorobami przewlekłymi, doprowadza do wzrostu popularności medycznych nośników (medical wearables). Według raportu Global Industry Analysts oczekuje się, że do 2020 r. światowy rynek wyrobów medycznych do użytku domowego wyniesie 4,5 miliona dolarów.

Z tego względu powołano IEC/TC 124, który rozpocznie prace nad normalizacją nośników medycznych i technologii z nimi związanej.

A co z kradzieżą tożsamości?

Choć dane biometryczne są unikalne dla osób fizycznych i są logicznym wyborem jeśli chodzi o bezpieczeństwo dostępu i kontroli, to jednak niczego nie można uznać za 100% bezpieczne. Karty, hasła i osobiste numery identyfikacyjne można anulować lub zmienić w przypadku utraty, zagubienia lub kradzieży, podczas gdy z odciskami palców, które zostały skopiowane i niewłaściwie wykorzystane, już tak postąpić się nie da. Ponadto informacje biometryczne są przechowywane w bazach, które muszą być chronione przed wszelkimi potencjalnymi naruszeniami bezpieczeństwa. Jeśli ta technologia ma się rozpowszechnić, to kwestie problematyczne muszą zostać rozwiązane.

Oprogramowanie i sprzęt w samochodzie będzie wymagał ochrony. Wiele podkomitetów ISO/IEC JTC 1 przyczynia się do zmniejszenia takich zagrożeń, na przykład ISO/IEC JTC 1/SC 27 *IT Security techniques*. Duża liczba danych będzie wymieniana między aplikacjami na smartfonach a inteligentnymi panelami samochodowymi, które również będą integralną częścią Internetu rzeczy. Praca ISO/IEC JTC 1/SC 6 *Telecommunications and information exchange between systems* przyczynia się również do poprawy bezpieczeństwa danych.

Źródło: IEC etech magazine, Issue 03/2017
J.S.