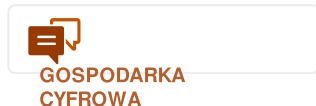


Objective Control for TAlker VErification

Wyniki w skrócie

Mechanizmy uwierzytelniania użytkowników na podstawie głosu mogą być wiarygodne i bezpieczne

Nowa platforma stworzona przez uczestników unijnej inicjatywy ma szansę sprawić, że technologia automatycznego rozpoznawania mówcy – czyli uwierzytelniania użytkownika na podstawie głosu – w końcu stanie się realną alternatywą dla haseł dostępu do urządzeń, usług i miejsc.



© SEA

Finansowani przez UE badacze zaprojektowali system OCTAVE – platformę do automatycznego rozpoznawania mówcy (ASV, Automatic Speaker Verification) umożliwiającą rzetelne i bezpieczne sprawdzanie tożsamości użytkowników na podstawie ich głosu.

„Naszym głównym celem było pozbycie się haseł ze wszystkich aplikacji i zwiększenie zaufania do technologii ASV” – mówi

Sebastiano Trigila, koordynator projektu i członek dyrekcji włoskiej fundacji Fondazione Ugo Bordoni (FUB).

Dla wielu osób konieczność pamiętania haseł do różnych urządzeń i usług jest bardzo frustrująca. A w przypadku firm jest również kosztowna: badania wskazują, że około 30% zapytań kierowanych do działów pomocy technicznej dotyczy odzyskiwania i resetowania haseł.

Zespoły zajmujące się rozwojem inteligentnych usług już teraz zaczynają myśleć nad niewymagającymi nadzoru człowieka rozwiązaniami, takimi jak systemy kontroli dostępu do wrażliwych obszarów budynku, które mogą wyeliminować systemy oparte na tokenach (np. inteligentne karty). Jednakże w przypadku biometrii głosowej istnieje wiele obaw dotyczących bezpieczeństwa, a w szczególności ryzyka podszywania się, co skutecznie hamuje wdrażanie tej technologii.

„Chcieliśmy, aby nasz system był odporny na ataki zarówno zwykłe, polegające na przesłaniu do ASV nagranego głosu, jak i te bardziej wyrafinowane z użyciem syntezy mowy” – wyjaśnia Trigila. „Platforma OCTAVE jest dowodem na to, że ataki takie można skutecznie wykrywać i odpierać”.

Bezpieczeństwo w chmurze

Przedsiębiorstwa korzystające z platformy OCTAVE nie muszą kupować własnych systemów ASV – mogą korzystać z ASV udostępnianych w jako usługi chmurowe na zaufanych platformach prowadzonych przez wybrane firmy trzecie. Kiedy przedsiębiorstwo, działające jako dostawca usług, chce uwierzytelnić użytkownika, może skorzystać z takiej platformy zewnętrznej.

Aby zapewnić bezpieczeństwo danych, zespół OCTAVE zastosował system rozproszony. Dane użytkowników nie są przechowywane na jednym serwerze, ale w całej chmurze obsługiwanych przez niezależne firmy serwerów komunikujących się ze sobą za pośrednictwem standardowych i zabezpieczonych protokołów. Dane osobowe i dotyczące profilu usługi pozostają na serwerze dostawcy, zaś przez system OCTAVE przesyłane są tylko próbki głosowe i automatycznie generowany numer ID. Po wygenerowaniu i zapisaniu wzorców głosu próbki są natychmiastowo usuwane.

System nie do złamania

„Nawet w przypadku kradzieży wzorca głosu trzeba jeszcze złamać szyfr oparty na wielu kluczach i włamać się do łańcucha serwerów. Dopiero wówczas można podszyć się pod inną osobę” – zauważa Mauro Falcone, techniczny lider projektu i starszy badacz w FUB. Innym innowacyjnym zabezpieczeniem jest kontrola prawdziwości głosu przed przesłaniem próbki do weryfikacji, co pozwala wykrywać próby podszywania się na bardzo wczesnym etapie.

Przeprowadzone w lecie 2017 roku testy – z użyciem systemu kontroli dostępu do obszarów zastrzeżonych mediolańskiego lotniska Linate i systemu wsparcia dla klientów banku internetowego Findomestic – dowiodły, że użytkownicy uważają to przełomowe rozwiązanie za łatwe w obsłudze. Na podstawie danych z testów standardowych, w tym testu porównawczego zabezpieczeń ASV 2017 przed fałszerstwem, stwierdzono, że system sprawdza się doskonale nawet w obecności

szumów w tle.

„Rezultaty każdego przeprowadzanego przez nas testu mieszczą się w pierwszej piątce najlepszych wg dostępnej dokumentacji wyników. Jak dotąd innym zespołom badawczym udało się zaledwie przetestować bazowe algorytmy, podczas gdy my sprawdziliśmy cały system” – twierdzi Falcone.

Uczestnicy projektu OCTAVE opublikowali wiele artykułów w czasopismach naukowych i zainspirowali inny zespół badawczy z Finlandii do przeprowadzenia badań kontynuacyjnych. Komerccjalni partnerzy projektu – firmy ValidSoft i Atos Spain – planują już wkrótce włączyć usługę do swojej oferty. Trigila z optymizmem myśli o przyszłości systemu ASV. „Ta technologia jest nie tylko potężna, ale również niemożliwa do złamania w kontekście chmury” – podsumowuje.

Słowa kluczowe

OCTAVE

biometria głosowa

automatyczne rozpoznawanie mówcy

ochrona przed podszywaniem się

hasła

inteligentne systemy

Znajdź inne artykuły w tej samej dziedzinie zastosowania



Najszybszy na świecie trójwymiarowy skaner stóp toruje drogę rewolucji obuwniczej

7 Grudnia 2017





DETECTOR: broń przeciwko pasażerom na gapę

3 Sierpnia 2020



Cyfryzacja fizycznych punktów sprzedaży

3 Stycznia 2020



Technologia łańcucha bloków sprawia, że bezpieczne, tanie i proste płatności stają się ogólnodostępne

26 Czerwca 2020



Informacje na temat projektu

OCTAVE

Identyfikator umowy o grant: 647850

[Strona internetowa projektu](#) 

DOI

[10.3030/647850](https://doi.org/10.3030/647850) 

Projekt został zamknięty

Finansowanie w ramach

Secure societies - Protecting freedom and security of Europe and its citizens

Koszt całkowity

€ 5 208 985,00

Wkład UE

€ 4 406 116,00

Koordynowany przez

Data podpisania przez KE

1 Maja 2015

FONDAZIONE UGO BORDONI

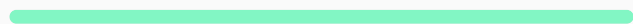


Data rozpoczęcia

1 Czerwca 2015

Data zakończenia

31 Lipca 2017



Ostatnia aktualizacja: 6 Grudnia 2017

Permalink: <https://cordis.europa.eu/article/id/210725-user-authentication-by-voice-can-be-robust-and-secure/pl>

European Union, 2025