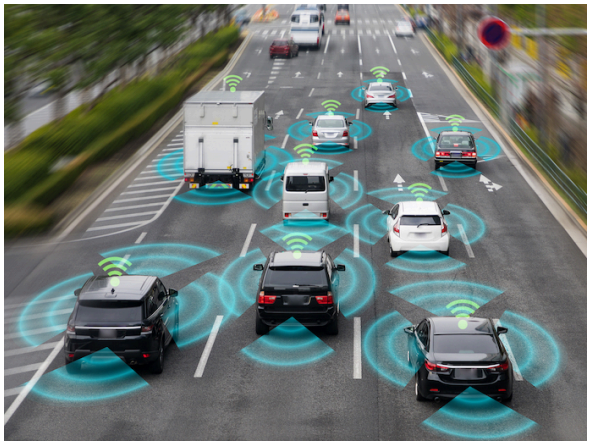
Artificial Intelligence based cybersecurity for connected and automated vehicles

Wyniki w skrócie

Zwiększanie cyberbezpieczeństwa inteligentnych pojazdów

Z uwagi na to, że samobieżne, połączone inteligentne pojazdy przewożą coraz więcej osób i towarów, ich bezpieczeństwo ma coraz większe znaczenie. Zespół projektu CARAMEL tworzy rozwiązania z zakresu bezpieczeństwa cybernetycznego pojazdów, uwzględniające ryzyko, oparte na procesach i obejmujące wszystkie etapy – od projektu do wdrożenia.

BEZPIECZEŃSTWO



© Metamorworks/Shutterstock.com

Postępy w dziedzinie łączności i sztucznej inteligencji zaowocowały stworzeniem wielu inteligentnych funkcji w nowoczesnych pojazdach, a wraz z nimi powstały wyrafinowane cyberprzestępstwa wykorzystujące luki w zabezpieczeniach.

W skrajnych przypadkach złamanie cyberzabezpieczeń skutkuje zagrożeniem bezpieczeństwa pasażerów, pieszych, innych pojazdów i infrastruktury krytycznej. Częściej prowadzi do kradzieży pojazdu lub wycieku wrażliwych danych.

„Pojazdy stają się »centrami danych na kółkach«, co sprawia, że często są celami ataków. Jeśli bezpieczniejsze, inteligentniejsze i bardziej ekologiczne pojazdy mają stać się powszechne, to muszą być godne zaufania i cyberbezpieczne”, mówi Jordi Guijarro Olivares, koordynator projektu CARAMEL.

W ramach projektu finansowanego ze środków UE, koordynowanego przez centrum badań i2CAT Foundation, opracowano strategie uzupełniania kluczowych luk w zabezpieczeniach w czterech priorytetowych obszarach operacyjnych.

„W ramach naszego systemu »Cooperative Situational Awareness« rozwijamy cyberbezpieczeństwo stosując jednolite podejście do ochrony i wykorzystując czujniki pojazdów do budowania odporności. Nie ograniczamy się do zaradzania skutkom cyberataków", wyjaśnia Peter Hofmann, koordynator techniczny projektu CARAMEL.

Cztery filary bezpieczeństwa cybernetycznego

Podejście obrane w projekcie CARAMEL polegało na wprowadzeniu technologii cyberbezpieczeństwa opartej na czterech filarach zarówno w pojazdach, jak i w wewnętrznej infrastrukturze. Pierwsze trzy zostały przetestowane w siedzibie firmy Panasonic na początku tego roku.

W ramach pierwszego filaru, czyli Mobilności autonomicznej, zastosowano techniki uczenia maszynowego w celu wykrywania zagrożeń związanych z interfejsem radiowym i czujnikami, by chronić autonomiczne funkcje pojazdów (takie jak rozpoznawanie scenerii) oraz ich czujniki pokładowe (takie jak kamery, czujniki LiDAR i GPS).

Opracowano również nowe urządzenie zabezpieczające przed cyberatakiem, będące częścią pokładowej jednostki sterującej, które przesyła analizę danych pokładowych do dalszego przetwarzania lub wizualizacji.

Do trenowania i walidacji uczenia maszynowego wykorzystano zarówno zbiory danych symulacyjnych i rzeczywistych, pochodzące ze źródeł publicznych oraz dostarczone przez partnerów.

„Ostateczna wersja demonstracyjna przewyższyła nasze oczekiwania, okazała się odporna na wiele typów ataków o różnych stopniach nasilenia. Nasze urządzenie zapobiegające cyberwłamaniom z powodzeniem wykryło ataki na czujniki, takie jak fałszowanie lokalizacji i zakłócanie odczytu znaków drogowych, przez co zachowana została świadomość sytuacyjna pojazdu", dodaje Guijarro Olivares.

W ramach drugiego filaru, nazwanego Połączoną mobilnością, koncentrowano się na wykrywaniu ataków na połączone pojazdy. Zespół wdrożył protokoły vehicle-to-everything (V2X), które umożliwiały komunikację między pojazdami oraz z urządzeniami komunikacyjnymi znajdującymi się na poboczu.

Opracowano także rozwiązanie, dzięki któremu pojazdy mogą współpracować ze sobą w celu identyfikacji ataków polegających na zafałszowaniu lokalizacji GPS, aktywując w odpowiedzi zaawansowane funkcje ochrony prywatności.

Stworzono również architekturę, za pomocą której połączono alarmy pojazdów z serwerami w chmurze. Po wykryciu ataku uruchamiane są protokoły bezpieczeństwa oraz monitorowanie aktywności.

W ramach trzeciego filaru, Elektromobilności, stworzono oparte na chmurze i sztucznej inteligencji silniki detekcyjne do zdalnego wykrywania cyberataków na stacje ładowania, poprzez rozpoznawanie anomalii w komunikacji pomiędzy stacją a jej zdalnym zapleczem.

„Wiele stacji ładowania jest wyposażonych w przestarzały sprzęt lub oprogramowanie, więc nie spełnia najnowszych standardów bezpieczeństwa. Odkryliśmy, że zastosowanie metod statystycznych, takich jak współczynnik korelacji Pearsona i las losowy, znacznie zmniejszyło złożoność modeli uczenia maszynowego potrzebnych do wykrywania anomalii i ochrony stacji”, tłumaczy Petros Kapsalas, kierownik badań projektu CARAMEL.

Czwarty filar, czyli Pojazd zdalnie sterowany, jest nadal rozwijany przez południowokoreańskich partnerów projektu, a prace będą finansowane jeszcze przez rok.

Zespół ten pracuje nad projektem niezbędnej architektury przetwarzania danych i rozwiązania do wykrywania zagrożeń, aby zdalnie sterowane pojazdy 5G były bezpieczniejsze.

Cyberbezpieczeństwo nowej generacji

Transport jest częścią europejskiej infrastruktury krytycznej, dlatego został objęty szczególną ochroną w czasach kryzysu i jest uważany za główny filar europejskiej strategii bezpieczeństwa cybernetycznego.

Jak twierdzi Guijarro Olivares, „osiągnięcia projektu CARAMEL wyraźnie przyspieszą rozwój nowej generacji cyberbezpieczeństwa autonomicznych, połączonych i elektromobilnych pojazdów. Aby jednak podmioty europejskie mogły z nich skorzystać, należałoby najpierw zająć się kwestią niedopasowania prawodawstwa do potrzeb przemysłu”.

Słowa kluczowe

CARAMEL, bezpieczeństwo, inteligentny, samobieżny, połączony, cyberbezpieczeństwo, sztuczna inteligencja, uczenie maszynowe, cyberprzestępczość, dane, 5G

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Cyfryzacja sektora gospodarki wodnej

Gdy technologia zapewnia ochronę

Zwiększanie bezpieczeństwa urządzeń internetu rzeczy dzięki rezygnacji ze statycznych danych uwierzytelniających

Wzmocnienie odporności szpitali na zagrożenia

Informacje na temat projektu

CARAMEL

Identyfikator umowy o grant: 833611

Strona internetowa projektu

DOI
10.3030/833611

Projekt został zamknięty

Data podpisania przez KE
27 Września 2019

Data rozpoczęcia
1 Października 2019

Data zakończenia
30 Czerwca 2022

Finansowanie w ramach
INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Koszt całkowity
€ 7 033 655,10

Wkład UE
€ 4 998 503,51

Koordynowany przez
FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATALUNYA
Spain

Ostatnia aktualizacja: 4 Listopada 2022

Permalink: https://cordis.europa.eu/article/id/442445-making-smart-vehicles-more-cybersecure/pl