

Beveiliging van het Internet of Things – Automotive

Inleiding:

In de komende jaren gaan voertuigen op de weg op flinke schaal met elkaar communiceren om de verkeersveiligheid en de doorstroming te optimaliseren. Fabrikanten en overheden wereldwijd investeren al jaren enorm in zowel de technologie als de toepassingen van Connected voertuigen (V2X). Nederland ambieert een koploperpositie in zowel de technologie als de toepassingen van V2X en heeft diverse publiek private samenwerkingsprogramma's hiertoe opgericht en gefinancierd (AutomotiveNL, DITCM, Connecting Mobility, Beter Benutten, EU Truck Platooning Challenge, ITS Corridor, SPITS).

De security uitdaging:

Voor de betrouwbaarheid van het communicatieverkeer tussen voertuigen en hun omgeving (het V2X-verkeer) is door de industrie een standaard ontwikkeld op het gebied van security en privacy. Hierdoor kunnen enerzijds de berichten vertrouwd worden (security) en anderzijds individuele voertuigen niet gevolgd (privacy). Waar nog een flinke weg is te gaan is een monitoringssysteem dat onbetrouwbare voertuigen of slecht-functionerende voertuigzenders kan detecteren en diagnostiseren t.b.v. opsporing en handhaving. Potentiële use cases van misbruik van V2X zijn o.a. de lokale verstoring van GPS signalen of de lokale overbelasting van het radiospectrum voor V2X (5,9 GHz band op basis van Wifi-P).

Het initiatief:

Bijeenbrengen van enkele partijen uit de Triple helix om de probleemstelling te verkennen en het ontwikkelen van een effectieve (deel)aanpak van de probleemstelling in research, ontwikkeling en pilots t.b.v. de potentiële full deployment in de Europese markt van 500 miljoen voertuigen.

Samenwerkingsvorm:

- Triple helix van AutomotiveNL en de HSD (The Hague Security Delta) in nauwe samenwerking en samenwerking met een kernteam van de Smart Mobility Ronde tafel Security (<http://www.ditcm.eu/its-round-tables/security>) dat is aangesloten bij de internationale werkgroepen voor ITS Security (EC, ETSI, UNECE).

Contactpersonen:

- AutomotiveNL – Bram Hendrix
- HSD - Bert Feskens
- Smart mobility Ronde tafel Security – Gilles Ampt

CONCEPT – 25 juli 2016



Literatuur probleemstelling:

- Detecting Sybil attacks in Vehicular Networks, Al-Mutaz *et al.*, *Journal of Trust Management* 2014, 1:4 <http://www.journaloftrustmanagement.com/content/1/1/4>
- Blocking Epidemic Propagation in Vehicular Networks, Basaras *et al.*, *2016 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)* <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7429049&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel7%2F7425033%2F7429033%2F07429049.pdf%3Farnumber%3D7429049>
- US DOT – Readiness of V2V for application www.nhtsa.gov/.../V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf