VAS
institute



Rapport nº 2022-R-08-NL

Cyberveiligheid bij geconnecteerde voertuigen

SERVICE PUBLIC FÉDÉRAL
MOBILITÉ ET TRANSPORTS

CYBERVEILIGHEID BIJ GECONNECTEERDE VOERTUIGEN

Rapport nº 2022 - R - 08 - NL

Auteurs: Dagmara Wrzesinska, John-John Deleuze

Review: Lina Kolesnikova, Annelies Develtere

Verantwoordelijke uitgever: Karin Genoe

Uitgever : Institut Vias

Publicatiedatum: 4/01/2022

Wettelijk depot: /2022/0779/22

Gelieve op de volgende manier naar dit document te verwijzen:: Wrzesinska, D., & Deleuze, J.J (2022). Cyberveiligheid Bij Geconnecteerde Voertuigen. Brussel, België: Vias Institute – Kenniscentrum verkeersveiligheid.

Ce rapport est également disponible en français sous le titre: Cybersécurité de la conduite connectée.

This report includes a summary in English.

Dankwoord

Deze studie werd gefinancierd door de Federale Overheidsdienst Mobiliteit en Vervoer.

De auteurs en het Vias-institute wensen de volgende personen en organisatie te bedanken voor hun bijdrage aan deze studie:

De Hogeschool HOWEST voor hun enthousiast engagement tijdens het project en hun uitnodiging om deel te nemen aan hun stageprogramma, met vooral een bijzondere dank voor **Preben Ver Eecke**, die ons op een vriendelijke wijze ondersteunde en de samenwerking coördineerde.

Gauthier Willaerts, student in de toegepaste informatica aan de Hogeschool HOWEST, voor zijn buitengewoon vlotte en aangename samenwerking, en die de onderzoeksgroep met zijn cruciale expertise vervolledigde en die tevens een grote flexibiliteit vertoonde tijdens de moeilijke periode met de COVID-beperkingen.

De uiteindelijke verantwoordelijkheid voor de inhoud van dit rapport blijft bij de auteurs.

Inhoud

Summary 5
1 Achtergrond 6
2 Standaardisering 7
2.1 Norme ISO/SAE 21434 8
2.2 UNECE WP.29 8
2.3 Verband tussen de ISO-norm en de WP.29-regelgeving 9
3 Gevolgen van V2X 11
3.1 V2X- communicatietechnologie 11
3.2 V2X uitdagingen en vereisten 12
3.3 V2X-veiligheidsoplossingen 13
4 Wie zijn de hackers? 15
4.1 Ethische hackers (white hat) 15
4.2 Malafide hackers (black hat) 15
4.3 Hackers uit de grijze zone (grey hat) 15
5 Hoe breken ze in? 16
5.1 Bedreigingstaxonomie 16
5.2 Aanvalsoppervlakken 17
5.3 Aanvalsvectoren 18
5.4 Gevolgen en scenario's 20
5.5 Toegepaste aanvalsscenario's 22
5.5.1 Rolljamaanval 22
5.5.2 Infotainmentaanval 24
5.5.3 OBD II-aanval 25
5.5.4 TPMS-aanval 27
6 Bekende pogingen uit het verleden 31
7 Tegenmaatregelen 33
8 Aanbevelingen 35
9 Woordenlijst 38

Summary

The increasing connectivity of the vehicles results in a rise of automotive cyberattack and a growing number of threats across the entire automotive supply chain. With the increasing number of connected vehicles, increase of vulnerabilities is expected to follow. Cyber incidents with malicious intent in 2020 accounted for majority of the attacks (54,6%) and keep growing exponentially. The outbreak of COVID19 pandemic, imposed even more challenges and increased the exposure to safety breaches.

One of the most efficient way to ensure the cybersecurity of the vehicle over its entire life time – the *security by design* approach – is reflected in the growing number of standardization in the domain. Notably, ISO/SAE 21434 and the regulation of UNECE WP.29 on cybersecurity have been introduced to the market.

In this study, we lay the main focus on the threats related to Vehicle-to-Everything (V2X) communication, which supports the rise of connected and autonomous vehicles. It allows use cases such as vehicle platooning, cooperative collision avoidance and remote driving which results in an improved road safety and traffic flow thanks to real-time data exchange. To support such exchange, two main technologies are used: Dedicated Short Range Communication (DSRC), known as ITS-G5 in Europe, and hand Cellular V2X (C-V2X) using LTE, 4G and 5G in the near future. Different types of resulting challenges as well as possible countermeasures are discussed in this report.

We analyse 10 different types of possible cyberattacks, 12 attack surfaces and 5 attack vectors. Based on this framework, we constructed 4 attack scenarios that we applied on the vehicle from our own fleet. Two of them we were able to execute successfully.

Lastly, the 4-level countermeasure framework for ensuring cybersecurity is discussed as well as some possible technological solution that can reduce the risk of security. Additionally, we propose 5 major focus areas for the authorities to invest their efforts in the future.

1 Achtergrond

Uit de resultaten van ons vooronderzoek was naar voren gekomen dat de toenemende connectiviteit in de autosector geleid had tot een stijging van het aantal cyberaanvallen tegen auto's. In dat verband wordt het dringend tijd dat de Original Equipment Manufacturiers (OEM's) van cyberveiligheid een prioriteit maken in hun organisatie, om de veiligheid en beveiliging van de weggebruikers te garanderen. Het aantal cyberincidenten van malafide hackers is in 2020 wel met zo'n 3% achteruitgegaan vergeleken met het jaar daarvoor, maar achter de meeste aanvallen zit nog altijd kwaad opzet (54,6%). 2020 heeft de autosector opgezadeld met tal van nieuwe uitdagingen die een bijkomende impact hebben op de cyberveiligheid ervan:

- OEM's en Tier 1-bedrijven hadden af te rekenen met een verstoring van hun toeleveringsketen als gevolg van de lockdown in een aantal landen en de afnemende vraag naar voertuigen. Dit leidde tot het stilleggen van fabrieken, onder meer bij General Motors, Volkswagen of BMW, en tot miljarden misgelopen inkomsten. Toch kunnen de OEM's sterker uit deze crisis komen door hun structuren en operationele processen te herdenken en mits ze focussen op nieuwe opportuniteiten om de vraag te stimuleren via elektrisch, geconnecteerd en gedeeld rijden. Bovendien zullen voertuigen op de wegen in de EU vanaf 2022 verplicht over Advanced Driver Assistance Systems (ADAS) moeten beschikken die ondersteund worden door V2X-communicatietechnologieën (Vehicle-to-everything) die het aantal kwetsbare plekken en toegangspunten flink doen toenemen en daarmee naar verwachting ook de interesse van hackers.

- Veel van de incidenten in cyberveiligheid bij auto's zijn te verklaren vanuit een gebrek aan expertise op het vlak van cyberveiligheid bij de OEM's. Een dramatisch gevolg van COVID-19 is zijn impact op het IT-budget van de ondernemingen, als gevolg van de onzekere inkomsten voor de lopende jaren. Een $(ISC)^2$-onderzoek toont aan dat de gezondheidscrisis de expertisekloof nog vergroot heeft. Daar zijn uiteenlopende verklaringen voor, waaronder het verlagen van het IT-budget, of personeel bij cyberveiligheid dat gedetacheerd werd naar andere IT-functies omdat er meer telewerkers waren en het moeilijk bleek om gekwalificeerde mensen te rekruteren. De kloof wordt des te groter als we denken aan het toegenomen aantal cyberaanvallen. We zagen een toenemend aantal OEM's, zoals Ford, GM, Tesla en Daimler bug-bounty-programma's lanceren in een poging om iets aan die kloof te doen. Bug-bounty-programma's bijvoorbeeld, zijn een soort wedstrijden die organisaties opzetten om bressen in hun cyberveiligheid te laten opsporen, in ruil voor een financiële vergoeding.

- In 2020 werden meer dan 207 nieuwe cyberincidenten met auto's gemeld, een evenaring van het record, met als resultaat een toename van 34% vergeleken met 2019. Het is van belang om op te merken dat niet alle incidenten officieel gemeld werden en dat veel van de illegale cyberhackingactiviteiten plaatsvinden op het darkweb.

- Het aantal aanvallen tegen servers is sinds 2019 met 73% gestegen. Het gaat daarbij om aanvallen tegen telematica-, data- en webservers, vanaf een (lange) afstand en met goedkope middelen. Servers aanvallen is een praktijk die we ook kennen uit andere sectoren, maar die almaar vaker de autosector treft. Dit soort aanvallen kan de hacker een ongeoorloofde toegang verschaffen tot verscheidene voertuigen tegelijk. Dat was het geval in augustus 2020, toen een hacker via de commando- en controleserver toegang kreeg tot het hele Tesla-wagenpark.

2 Standaardisering

We identificeerden zo'n 20 normeringen en regelgevingen die van toepassing kunnen zijn op het domein van de cyberveiligheid bij auto's en hebben die opgenomen in de onderstaande lijst. Sommige ervan dateren van vóór dat de autosector specifiek betrokken was bij de cyberdreigingen. Aangezien ze echter opgesteld werden met het oog op de beveiliging en veilige werking van elektronische onderdelen of communicatieprotocollen zijn ze ook van belang voor de productie van veilige en beveiligde geconnecteerde voertuigen.

Vandaag is het interessant om te focussen op de ISO/SAE 21434-norm en de regelgeving uit UNECE (United Economic Commission for Europe) WP.29 over cyberveiligheid. Beide worden immers binnenkort gepubliceerd en zullen op korte termijn van kracht worden.

Standard code	Year	Full name	Link
IATF 16949	2016	Automotive Quality Management System	link
IEC 62443-2-1	2010	Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program	link
ISO 9001[1]	2015	Quality Management Systems — Requirements	link
ISO 14229-1:2020	2020	Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer	link
ISO 14230-2:2016	2016	Road vehicles — Diagnostic communication over K-Line (DoK-Line) — Part 2: Data link layer	link
ISO 15765-2	2016	Standard for Sending Data Packets Over a CAN-Bus -> Road Vehicles: Diagnostic Communication over Controller Area Network (DoCAN)	link
ISO 17458-1	2013	FlexRay Communications System	link
ISO 20078	2021	Extended vehicle (ExVe) web services	link
ISO 21434	2021	Road vehicles — Cybersecurity Engineering	link
ISO 26262- 3	2018	Road vehicles — Functional safety — Part 3: Concept phase -> Classification of hazardous events	link
ISO 26262-1:2018	2018	Road vehicles — Functional safety — Part 1: Vocabulary	link
ISO 29147	2018	Information technology — Security techniques — Vulnerability disclosure	link
ISO 31000:2019	2019	RISK MANAGEMENT: Assessment Techniques	link
ISO/IEC 27001	2018	INFORMATION SECURITY MANAGEMENT: Information technology — Security techniques — Information security management systems — Overview and vocabulary	link
ISO/IEC DIS 18045	2020	Information Security, Cybersecurity and Privacy Protection — Evaluation criteria for IT security — Methodology for IT security evaluation **(work in progress)**	link
ISO/IEC/IEEE 12207:2017	2017	Systems and Software Engineering — Software life cycle processes **(work in progress)**	link
ISO/IEC/IEEE 15288:2015	2015	Systems and Software Engineering — System life cycle processes **(work in progress)**	link

PAS 1885	2018	The Fundamental Principles of Automotive Cyber Security	link
PAS 11281	2018	Connected Automotive Ecosystems – Impact of Security on Safety – Code of practice	link
SAE J2602	2012	LIN Network for Vehicle Applications: Minimum Standard Level of Performance (seat belts, air conditioning, door locks etc.)	link
SAE J3061	2016	Cybersecurity Principles and Guidance for Cyber-Physical Vehicle Systems	link
SAE J3101	2020	Common Requirements for Security to be implemented in Hardware for Ground Vehicles	link
ISO/CD 24089	2020	Road vehicles – Software engineering	link

2.1 Norme ISO/SAE 21434

Verwacht wordt dat de samenwerking tussen SAE en ISO een referentie zal worden voor een cyberveilige toeleveringsketen in de autosector. De norm verscheen in 2020 voor openbare raadpleging en ondergaat momenteel de reviews van de technische comités. De definitieve versie van de norm is halverwege 2021 verschenen. ISO/SAE 21434 komt boven op ISO 26262 '*Wegvoertuigen – Functionele veiligheid'* als veiligheidsgerelateerde norm in het proces van het ontwikkelen van voertuigen. Veel ondernemingen waaronder OEM's, hardwareleveranciers, actoren in cyberveiligheid en andere werken aan die normen. De norm heeft uiteenlopende doelstellingen:

1	Hij brengt een globale norm voor de autosector tot stand met een gemeenschappelijke terminologie op het vlak van cyberveiligheid in de engineering
2	Hij bepaalt de minimumvereisten voor processen en activiteiten in cyberveiligheid bij engineeringactiviteiten
3	Hij bevordert de samenwerking tussen de verschillende stakeholders doorheen de toeleveringsketen voor de autosector
4	Hij bekijkt voertuigen over hun hele levenscyclus: van de ontwerpfase over productie, verkoop, onderhoud, tot de ontmanteling

Hoofddoelstelling is om via het ontwerp de veiligheid te garanderen en de ontwikkeling van veilige voertuigen te verzekeren, maar er zitten ook doelstellingen op het vlak van cyberveiligheid in opgenomen gericht op de hele levenscyclus van het voertuig.

2.2 UNECE WP.29

Op 25 juni 2020 heeft het 'World Forum for Harmonization of Vehicle Regulation' WP.29, een werkgroep van de 'United Nations Economic Commission for Europe' (UNECE), de allereerste reglementering rond cyberveiligheid bij auto's uit de geschiedenis goedgekeurd: UNECE-reglement (UNR) nr. 155 en 156.

- UNR 155: Dit reglement legt de uiteenlopende vereisten vast waaraan OEM's moeten voldoen om hun Cybersecurity Management System (CSMS) goedgekeurd en gecertificeerd te krijgen. Om de goedkeuring te verkrijgen moeten OEM's en hun leveranciers het bewijs leveren van een cyberdreigingsanalyse en de implementatie van tegenmaatregelen. Het reglement is erop gericht om uiteenlopende cyberactiviteiten mogelijk te maken, van risicomanagement tot penetratietesten,

detectie van en reageren op incidenten, dreigingen bewaken, enz. verspreid over de hele levenscyclus van het voertuig. Het reglement berust op de norm ISO 21434. Aangezien hier de hele levenscyclus bekeken wordt, zou een aanpak van het cybersysteem dat zich beperkt tot de OEM wel eens ontoereikend kunnen blijken.

- UNR 156: Goedkeuring van de cyberveiligheid van een voertuig wat de software update en het software update management system (SUMS) betreft. Hiermee wil men tot veilige en beveiligde software-updates komen door een wettelijke basis in te voeren voor de zogeheten OTA-updates (over-the-air) van de software aan boord van het voertuig. Dit reglement heeft zin in het licht van de voortdurende evolutie van de optiemarkt voor softwaregebaseerde voertuigupgrades.

De beide reglementen leggen vereisten en maatregelen vast in 4 onderscheiden disciplines:

- beheren van de cyberrisico's die een voertuig oplevert;
- voertuigen beveiligen via het ontwerp ('by design'), om de risico's over de waardeketen tot het minimum te beperken;
- detecteren van en reageren op veiligheidsincidenten in een wagenpark;
- aanleveren van veilige en beveiligde software-updates door het invoeren van een wettelijke basis voor de zogeheten OTA

Deze regelgeving zal op korte termijn een impact hebben voor de autosector, aangezien OEM's verplicht worden om eraan te voldoen. Tegen juli 2022 moeten nieuwe voertuigen geproduceerd worden overeenkomstig UNR 155 en 156 om in de lidstaten verkocht te mogen worden. En vanaf juli 2024 zal een cyberveiligheidsgoedkeuring vereist zijn voor nieuw geproduceerde voertuigen. Deze deadlines liggen in de nabije toekomst. OEM's moeten nu dus met de voorbereiding beginnen om die tijdlijn te kunnen aanhouden.

2.3 Verband tussen de ISO-norm en de WP.29-regelgeving

De recentste versie van het UNECE-reglement nr. 155 vermeldt duidelijk dat ISO/SAE 21434 de implementatie ondersteunt van de vereisten van het CSMS in alle organisaties langsheen de hele toeleveringsketen. Tegelijk is ISO momenteel bezig met de ontwikkeling van een ISO/CD 24089-norm 'Ground vehicles – software engineering', ter ondersteuning van UNR 156. ISO/SAE 21434 en UNR 155 zijn daarom complementair en er beide op gericht om voertuigen op eenzelfde manier veiliger te maken. We zien uiteenlopende gelijkenissen tussen de beide:

- **Technologieneutraal**: geen van de reglementen is restrictief in het afbakenen van technische oplossingen of specifieke processen die OEM's in hun CSMS moeten opnemen. De reden daarvoor is dat een te descriptief reglement op het vlak van cyberveiligheid gevaarlijk kan zijn, gezien de constante evolutie van het cyberveiligheidslandschap en de nieuwe technologieën die hun intrede doen. Daarom beschrijven de vereisten veeleer processen of functies waarover een voertuig moet beschikken dan een specifieke technologie.

- **Levenscyclus en beveiligde toeleveringsketen:** we zien duidelijk dat de norm en de reglementen parallel ontwikkeld werden met mensen die bij de beide betrokken waren, aangezien ze twee belangrijke aspecten delen. Om te beginnen zijn ze beide revolutionair op het vlak van cyberveiligheid bij auto's, omdat ze OEM's verplichten cyberveiligheidsprocessen in te bouwen doorheen de hele levenscyclus van het voertuig, van de ontwikkeling tot de postproductiefase. Ten tweede stellen ze beide dat OEM's aansprakelijk zijn voor de veiligheid en het ontwerp van het product en als resultaat daarvan moeten garanderen dat ook hun toeleveringsketen veilig is. Ze moeten veiligheidsvereisten en -processen opgeven en controleren van Tiers vóór het integreren van componenten of software.

- **Aanpak:** beide hanteren een holistische aanpak van cyberveiligheid bij auto's door governancepraktijken en -processen te beschrijven op organisatorisch en operationeel niveau. UNR 155 benadert cyberveiligheid echter

ook op een praktischer niveau door in zijn Bijlage 5 uitgebreid praktijkvoorbeelden te beschrijven van dreigingen en de bijbehorende matigingsmaatregelen.

- **Veiligheid door het ontwerp:** dit concept 'security by design' staat centraal in het UNECE-reglement en de ISO-norm. De idee is om veiligheid te bekijken vanaf de vroege fase van het productontwerp zodat matigingsmechanismen van meet af aan geïntegreerd zijn en gemakkelijker af te stemmen op nieuwe dreigingen die opduiken tijdens de levenscyclus van het product. Dat proces vertrekt van een veiligheidsrisicoanalyse waarbij de financiële, operationele, privacy- en veiligheidsimpact in opeenvolgende stappen beoordeeld worden tot een aanvaardbaar risiconiveau. Toch impliceert het feit dat een product ontworpen, geïmplementeerd en getest is om 'veilig' te zijn (hoewel we allemaal weten dat 100% veilig niet bestaat), in geen enkele mate dat dit product ook in gebruik veilig zal zijn. De combinatie van product- en gebruiksgerelateerde veiligheidscontroles blijkt doorgaans een voordelige benadering.

- **CSMS:** vereisen de efficiënte implementatie van een Cybersecurity Management System in de organisatie.

Aspect	**ISO/SAE 21434**	**UNECE WP.29**
Doelstelling	Legt minimumcriteria op voor engineering van cyberveiligheid bij auto's	CSMS implementatie en typegoedkeuring van voertuigen
Gebruiker	OEM's, Tier 1, Tier 2	OEM's
Wettelijk	Niet bindend	Juridisch bindend
Datum	Midden 2021 (verschijning)	Januari 2021 (handhaving)
Plaats van handhaving	Overal	54 lidstaten
Type voertuig	Alle voertuigtypen voor de weg	Alle categorieën van 4-wielers
Betrokken fasen	De hele levenscyclus (ontwerp, engineering, productie, gebruik, onderhoud en ontmanteling)	Ontwikkeling, productie en postproductie
Mapping van cyberdreiging	Neen	Ja (Bijlage 5 van UNR155)
Geldigheid van CSMS	Eenmalig	Om de drie jaar

Zoals in andere sectoren al vastgesteld werd is het gedeelte van de productlevering in de levenscyclus belangrijk en een kritiek vertrekpunt. Het is behoorlijk gemakkelijk te bereiken aangezien het aantal spelers hier beperkt is. Veiligheid doordrukken naar het operationele gedeelte van de levenscyclus zou echter moeilijker kunnen uitvallen vanwege het grotere aantal betrokkenen. De productontwikkelaar (OEM) moet daarom het productaanbod beveiligen op basis van de goedgekeurde normen (veilige softwareontwikkeling, enz.). Behalve als we uiteenlopende gesloten ecosystemen (bv. één per OEM) willen invoeren, zoals dat van Apple, zullen we meer moeten nadenken over het operationele deel van de levenscyclus, hier postproductie genoemd. OEM's kunnen niet volledig aansprakelijk zijn voor wat in die operationele fase met hun product gebeurt. Ze bieden louter houvast bij een optimaal gebruik van hun product en leggen veiligheidscontroles op, in de mate dat de markt zulks accepteert. OEM's hebben, afgezien van gesloten ecosystemen type Apple, niet noodzakelijk iets te maken met het gebruik van hun producten en de bijbehorende operationele activiteiten. Als voorbeeld kunnen we denken aan 'militaire' voertuigen, waar we er niet van uitgaan dat de OEM het best geplaatst is om dergelijke gevoelige apparatuur te bedienen.

3 Gevolgen van V2X

Wij kunnen bij voertuigcommunicatie een onderscheid maken tussen twee typen: in-vehicle (IV) en vehicle-to-everything (V2X). Voor V2X-communicatie bestond de voorbije jaren een grote belangstelling omdat ze aansluit bij de komst van de geconnecteerde en zelfrijdende voertuigen en een beroep doet op draadloze technologieën, die door de communicatie van realtimegegevens de verkeersveiligheid en -doorstroming kunnen verbeteren. De uitrol van V2X biedt interessante mogelijkheden zoals konvooivorming, coöperatieve botsingvermijding en het rijden vanop afstand, die resulteren in een verbeterde verkeersveiligheid en -doorstroming, dankzij de realtime gegevensuitwisseling tussen voertuigen, wegeninfrastructuur, voetgangers en netwerk. Bij de V2X-communicatiesystemen kunnen vier hoofdtypen onderscheiden worden op basis van hoe het voertuig gegevens uitwisselt:

- **'Vehicle to vehicle' (V2V)**: gegevensuitwisseling tussen voertuigen om de snelheid en locatie van andere voertuigen te kennen. Dit helpt om voorspelbaarder en veiliger te kunnen rijden.

- **'Vehicle to infrastructure' (V2I)**: draadloze gegevensuitwisseling tussen het voertuig en de wegeninfrastructuur, zoals verkeerslichten, intelligente signalisatie of Road Side Unit (RSU). De doelstelling is om aan gegevens te komen over verkeer en weersomstandigheden en daardoor uiteindelijk het aantal verkeersongevallen en de bijbehorende kosten te beperken.

- '**Vehicle to pedestrian' (V2P)**: communicatie tussen een voertuig en een voetganger op sleutellocaties, zoals een kruispunt of oversteekplaats voor voetgangers. De primaire doelstelling van V2P is om kwetsbare weggebruikers te beschermen tegen aanrijding door voertuigen.

- '**Vehicle to network' (V2N)**: hiermee kunnen berichten doorgestuurd worden over verkeersongevallen of files die men tegemoet rijdt en over de weersomstandigheden. Wordt ook gebruikt voor in-vehicle-diensten, zoals mediastreaming.

3.1 V2X- communicatietechnologie

Een V2X-communicatiesysteem is sterk afhankelijk van het onderliggende communicatiesysteem dat voertuigen connecteert, onderling en met de transportinfrastructuur. Europa en Noord-Amerika hebben momenteel problemen met de uitrol van V2X, als gevolg van een gebrek aan duidelijkheid in de regelgeving en in de keuze van de communicatietechnologie waarop OEM's, mobiele netwerkoperatoren (MNO), dienstverleners en eigenaars en operatoren van infrastructuur zich zouden moeten baseren. De algemene vereisten voor een V2X-communicatiesysteem zijn hoge betrouwbaarheid, lage latentie voor veiligheidsgerelateerde toepassingen en een grotere bandbreedte en datasnelheid, voor toepassingen op het vlak van zelfstandig rijden.

Bij V2X-communicatie worden 2 hoofdtechnologieën gebruikt. Enerzijds Dedicated Short Range Communication (DSRC), in Europa gekend als ITS-G5, en anderzijds Cellular V2X (C-V2X) dat gebruik maakt van LTE, 4G en in de nabije toekomst ook 5G. De beide zijn gebaseerd op het 5,9 Ghz radiobandbreedtespectrum dat in 1999 is toegewezen voor gebruik met V2V en V2I. ITS-G5 was oorspronkelijk aangewezen als de standaardtechnologie voor ITS-diensten maar werd niet echt uitgerold, terwijl, volgens de CTO van NXP semiconductors, de technologie na jaren van ontwikkeling klaar is en we industrieklare, uiterst precieze en robuuste DSRC-chips hebben die tegen hacking bestand zijn.

In maart 2019 had een voorstel van de Europese Commissie tot doel om ITS-G5 te gaan gebruiken voor de korteafstandscommunicatie voor hulpdiensten en 3G en 4G als ITS-infrastructuur. Van de 28 lidstaten weigerden er echter 21 het voorstel omdat ze het niet eens waren met de keuze van de

korteafstandstechnologie. Hetzelfde debat over de twee technologieën leeft ook op de Amerikaanse en Aziatische markten. Het feit dat de prestaties van C-V2X met de tijd alleen maar kunnen verbeteren maakt het waarschijnlijk dat C-V2X op middellange termijn de referentietechnologie zal worden voor V2X-communicatie, maar zeker is dat nooit. In Europa worden verschillende initiatieven uitgerold, zoals het 'Smart Highway project' in Vlaanderen, om de prestaties van de twee technologieën te beoordelen.

De voornaamste voordelen van C-V2X zijn: efficiënt bij hoge snelheid en intensief verkeer, kostenefficiënte technologie, zelfbeheerd, uitgebreid bereik en hoge betrouwbaarheid, ingebouwde veiligheid van cellulaire netwerken. Een bijkomende troef van deze communicatietechnologie is dat ze gebruikmaakt van de bestaande cellulaire infrastructuur en bijgevolg minder RSU nodig heeft om geïnstalleerd te worden, hetgeen de kostprijs van de infrastructuur doet dalen. C-V2X en 5G zullen de ADAS-technologieën aanvullen en de uitbouw van zelfrijdende systemen ondersteunen.

De tabel vat de verschillende kenmerken van elke technologie samen. Een probleem dat we niet onvermeld mogen laten is het feit dat elke technologie haar fans heeft en dat in sommige onderzoekspapers dus belangenconflicten de kop kunnen opsteken. Bovendien kunnen de prestaties ook veranderen als gevolg van technologische verbeteringen

	DSRC	**C-V2X**
Chiptechnologie	ITS-G5	LTE/4G/5G (cellulaire modemtechnologie)
Frequentieband	5.9 GHz	
Berichtenstandaard	IEEE 802.11p	3GPP
Veiligheid	Digitale handtekening / cryptografie	
Bereik	Kort - 300m	Kort (direct) en lang (=cellulair netwerk/V2N)
Infrastructuurvereisten	Road Side Unit (RSU)	RSU + bestaande antennemast
Uitrol	Sinds 2017	Oorspronkelijke uitrol in 2021
Kenmerken	Snelle netwerkconnectiviteit Lage latentie (max. 150 ms) Beveiligd tegen hacking Gegevenssnelheid (tot 27 Mb/s)	Ultra-lage latentie (1-10 ms) Bredere bandbreedte/flexibiliteit (werkt in 3 spectra) Hoge betrouwbaarheid Achterwaarts compatibel (4G<->5G)

3.2 V2X uitdagingen en vereisten

Veel landen zetten almaar meer in op connectiviteit tussen voertuigen en transportinfrastructuur en V2X-compatibele voertuigen doen hun intrede als de nieuwste voertuiggeneratie, oorspronkelijk gebaseerd op DSRC dat slechts een onderbroken connectiviteit biedt. Nu lijkt C-V2X-communicatie de referentietechnologie voor de toekomst te worden. Geconnecteerde auto's wisselen data uit met de transportinfrastructuur, zoals RSU, om de verkeersveiligheid te verbeteren en om bij mobiliteitsdiensten een grotere efficiëntie te kunnen garanderen. Die toegenomen connectiviteit creëert echter nieuwe toegangspoorten voor en risico's op cyberaanvallen, die ernstige gevolgen kunnen hebben als de V2X-systemen niet naar behoren beveiligd zijn.

V2X-communicatie moet aan verschillende functionele vereisten voldoen, zoals een aanvaardbaar niveau van betrouwbaarheid, end-to-end latentie, bandbreedte, datasnelheid en bereik. Het aanvaardbare niveau voor elke functie hangt af van de toepassing en staat vermeld in dit 5G AA's-witboek.

V2X-communicatie moet betrouwbaar zijn en voldoen aan de volgende veiligheidsvereisten:

- **Authenticatie:** de primaire veiligheidsfunctie is de authenticatie van het bericht garanderen vóór de uitvoering.
- **Integriteit:** meteen na de authenticatiestap moeten de berichten die worden uitgewisseld tussen een voertuig en de wegeninfrastructuur beveiligd worden tegen elke ongeoorloofde wijziging, om de betrouwbaarheid en nauwkeurigheid ervan te garanderen. Elke wijziging van een bericht moet gedetecteerd worden.
- **Onweerlegbaarheid:** identiteit van de zender, locatie en tijd kunnen opgespoord worden. Dat kan aan de hand van de digitale handtekening.
- **Privacy:** afhankelijk van de lokale regelgeving moet V2X-communicatie anonimiteit, pseudonimiteit en privacy van de apparatuur van de gebruiker garanderen. De identiteit van kwaadwillige gebruikers moet echter opgespoord kunnen worden.
- **Beschikbaarheid:** garandeert dat systemen en informatie toegankelijk en bruikbaar zijn voor geautoriseerde individuen. In een V2I-omgeving bijvoorbeeld moeten RSU altijd beschikbaar zijn voor het garanderen van de betrouwbaarheid van een target.

Om te beginnen is het belangrijk om te onderstrepen dat de netwerkplanning en het uitrollen van C-V2X technologieën een grote impact zal hebben op het mogelijk misbruik van kwetsbare plekken en de aard van de dreigingen. Anderzijds bieden 3GPP-gestandaardiseerde 5G-systemen bepaalde veiligheidsdiensten die beproefd gebleken zijn op 4G, en andere diensten, waaronder encryptie, authenticatie, en gebruikersprivacy werden verbeterd. Anderzijds is 5G gebaseerd op een complexere structuur die nieuwe opportuniteiten voor aanvallen biedt en geen inherente bescherming biedt tegen DDos-aanvallen en stoorzenders. Om een beveiligde C-V2X-technologie te verkrijgen moet de netwerkoperator een beveilig netwerk uitbouwen en de hoeveelheid oppervlakteaanvallen beperken die de weggebruikers kunnen bedreigen.

Nogal wat soorten aanvallen kunnen de C-V2X-communicatie bedreigen. Ze zijn te vinden in deze paper maar de Sybil-aanval[1] is wellicht een van de gevaarlijkste omdat hij de integriteit van het bericht en de privacy van de identiteit in het gedrang brengt. De voornaamste aanvallen die met V2X te maken gebeuren vanop afstand. Ze worden beschreven in deel **Error! Reference source not found.**: valse berichten, wijziging van berichten, Sybil-aanvallen, DoS, afluisteren, lookalike-aanvallen, replay-aanvallen, black- en grey-holeaanvallen, locatie-opsporing.

3.3 V2X-veiligheidsoplossingen

Momenteel doen wat de veiligheid van V2X betreft nieuwe uiteenlopende technologieën hun intrede. Ze zijn gericht op een grotere veiligheid van communicatienetwerken, betere schaalbaarheid en een nauwkeurigere controle. Bepaalde technologieën bieden interessante opties om de veilige communicatie in een voertuignetwerk te garanderen, maar sommige daarvan berusten op complexe rekenoperaties die ongeschikt zouden kunnen blijken voor het beveiligen van grote hoeveelheden gegevens op korte tijd.

V2X-isolatie: deze veiligheidsmaatregel schrijft geen specifieke technologie voor maar heeft betrekking op de veiligheidsfunctie van de architectuur van de V2X-module. V2X-functies kunnen geïmplementeerd worden op een specifiek V2X ECU (Electronic Contor Unit) of een bestaand ECU. De eerste optie verdient de aanbeveling, ondanks de bijbehorende extrakosten, omdat kwetsbare plekken in de andere ECU's de veiligheid in het gedrang kunnen brengen.

[1] De aanvaller ondermijnt het reputatiesysteem van een netwerkdienst door een groot aantal valse identiteiten te creëren en te gebruiken om een buitenproportioneel grote invloed te verwerven

Vehicular Public Key Infrastructure (VPKI): het probleem van de veiligheidsvereisten voor V2X-communicatie werd aangepakt door met certificaten te werken die verdeeld en beheerd worden door PKI. Die certificaten maken het mogelijk dat de identiteit van de verzender niet langer vereist is. In plaats daarvan worden aan één voertuig voor de authenticatie van de berichten verscheidene pseudoniemen toegekend. Die veranderen geregeld om te voorkomen dat het voertuig getraceerd wordt. De PKI biedt ondersteunende diensten zoals authenticatie, aanleveren en intrekken van pseudoniemen en wordt beheerd door een certificatie-autoriteit.

Edge Computing: een methode waarbij de gegevens dicht bij de bron ervan verwerkt worden. Edge computing biedt een geschikte middelenallocatie, snellere verwerking en lage latentie. Een grote bandbreedte is mogelijk door de rekentaken te verdelen over verschillende edges.

Virtualiseren van de netwerkfunctie (NFV): verwijst naar het proces van het loskoppelen van de netwerkfuncties van geïntegreerde hardware om ze als virtuele machine op een software te doen draaien. Zo kunnen bepaalde veiligheidsfuncties zoals firewalls en inbraakdetectie aangeleverd worden en virusscanners kunnen aangeboden worden of op verzoek van de ene naar de andere knooppunt gemigreerd, om de globale veiligheid van de V2X-communicatie te verbeteren.

Blockchain: blockchaintechnologie wordt nog niet gebruikt voor het beveiligen van de gegevenstransmissie in een V2X-omgeving maar biedt een aantal sleuteleigenschappen die een verbeterde veiligheid en privacy mogelijk kunnen maken. Ze wordt beschouwd als een krachtig instrument om gegevens te beveiligen, aangezien ze een beroep doet op krachtige encryptie- en decryptie-algoritmen en intrinsiek de wijziging van om het even welk gegeven verhindert. Het gedecentraliseerde karakter van blockchain garandeert de vertrouwelijkheid en integriteit van de informatie. Toch brengt deze technologie voor het netwerk een niet te verwaarlozen werklast met zich mee en gaat ze in tegen de vereiste van lage latentie van de meeste V2X-toepassingen.
Softwaregedefinieerde netwerken: traditioneel netwerkbeheer is complex en foutgevoelig. Die problemen worden veroorzaakt door de strakke koppeling van het doorsturen van gegevens en de besturingslogica. Door die los te koppelen en programmeerbaarheid in te voeren, vereenvoudigen de taken van het netwerkbeheer en ontstaat een grotere flexibiliteit. In een V2X-omgeving kan dat gebruikt worden om gegevens dynamisch en efficiënt naar verschillende bestemmingen te rerouten.

Sterke draadloze gegevensencryptie: producenten garanderen dat de informatie die uitgewisseld wordt tussen de auto en de infrastructuur gebruikmaakt van de recentste encryptiealgoritmen, zodat ze niet door de aanvallers ontcijferd kan worden.

4 Wie zijn de hackers?

We onderscheiden vandaag uiteenlopende typen van hackers, afhankelijk van hun bedoelingen en de wettelijke aspecten van hun aanval. De autosector heeft onvoldoende mensen met expertise in cyberveiligheid. Daarom is het belangrijk om activiteiten te ontwikkelen om hackers op te sporen en te identificeren. Dan kan gepoogd worden hen te motiveren om voor de ondernemingen te werken en kwetsbare plekken op te sporen en af te schermen, liever dan de mogelijkheid van kwaadwillig gebruik open te laten. We kunnen drie soorten van hackers onderscheiden.

4.1 Ethische hackers (white hat)

Ethische hackers (white hat) zijn de 'goede' hackers. Ze breken in veiligheidssystemen in, zonder kwaadwillige bedoelingen te hebben. Ze doen dat van binnen de organisatie (bv. veiligheidsteam) of van buitenuit (bv. onafhankelijke onderzoeker). De legale kant van hun activiteit is wat hen van de anderen onderscheidt. Ze werken immers met de toestemming van de eigenaars van het systeem dat ze hacken. Toch dienen ze op te letten om geen regionale of nationale wetten te overtreden.

Hun voornaamste activiteiten zijn penetratietesten en kwetsbaarheidsbeoordelingen: kwetsbare plekken, kwaadwillige content, fouten en risico's vinden, door het testen van een computersysteem, de software of de IT-infrastructuur van een organisatie, met de bedoeling om toekomstige aanvallen te voorkomen. White-hat aanvallen dragen bij tot het verbeteren van de cyberveiligheid door het ontdekken van potentiële bedreigingen en worden dus door de sector verwelkomd. *Bug bounty-programma's* vormen een van de manieren om de bijdragen van ethische hackers aan te moedigen.

4.2 Malafide hackers (black hat)

Omgekeerd gebruiken malafide hackers hun knowhow met kwaadwillige bedoelingen. Ze staan bekend voor activiteiten als het schrijven van malware om veiligheidsprotocollen af te zwakken en te kunnen omzeilen. Ze profiteren van kwetsbare plekken in de beveiliging om ransomware en spyware binnen te loodsen. Hun motivatie kan financieel zijn, door de verkoop van persoonsgegevens van weggebruikers of het verstoren van de dienstverlening en kan tot de dood of tot verwonding leiden. Volgens het recentste cyberveiligheidsrapport van Upstream was 54,6% van de incidenten in 2020 veroorzaakt door malafide hackers.

4.3 Hackers uit de grijze zone (grey hat)

Dit derde type hacker zit in de zone tussen zwart en wit in. Ze dringen veiligheidssystemen binnen op zoek naar kwetsbare plekken zonder daarvoor de toestemming van de eigenaar te hebben, maar anders dan de malafide hackers hebben ze geen slechte bedoelingen. Hun motivatie is vaak persoonlijk. Ze lanceren een cyberaanval om een onderneming op haar kwetsbare plekken te wijzen, zonder schade te veroorzaken en vragen dan een bedrag om het in orde te brengen. Of soms verschaffen ze zich zo toegang tot een betalend product van de OEM.

5 Hoe breken ze in?

5.1 Bedreigingstaxonomie

Cyberaanvallen vallen uiteen in twee grote categorieën: fysiek of vanop afstand. Voor een fysieke aanval moet de hacker fysiek connecteren met het voertuig, terwijl bij een aanval vanaf een (korte of lange) afstand gebruikgemaakt wordt van netwerkconnectiviteit. Een fysieke aanval vereist meestal dure hardware en is niet discreet, omdat de aanvaller een fysieke toegang tot het voertuig moet hebben. Door de toegenomen connectiviteit werden aanvallen vanop afstand populairder en moeilijker te detecteren en tegen te gaan. Volgens Upstream Security waren tussen 2010 en 2020, 79,6% van alle aanvallen van dat type.

Er is geen centrale taxonomie van cyberaanvallen, maar Bijlage 5 bij WP.29 UN R155 identificeerde 69 verschillende aanvalswegen die ingedeeld werden in 7 cyberdreigingen en kwetsbaarheidscategorieën. Omdat OEM's zullen moeten aantonen hoe ze de in dit document opgesomde cyberdreigingen matigen, om CSMS-compliant verklaard te kunnen worden, geven we hieronder uit die bijlage de hoofdcategorieën van aanvallen:

- **Spoofingaanval** — wanneer de indringer een valse identiteit gebruikt of nepgegevens verstuurt. De indringers versturen ongeautoriseerde berichten met valse informatie om de voertuigcommunicatie te verstoren.
- **Jammingaanval** — wanneer ruis op het radiosignaal de frequentie van de communicatie verstoort, met als bedoeling om de V2X-communicatie te blokkeren of te hinderen.
- **Masqueradeaanval** — wanneer binnengedrongen wordt onder een valse identiteit, zoals een netwerkidentiteit, om ongeoorloofde toegang tot het voertuig te krijgen zonder een geldige toegangsauthenticatie.
- **Afluisteraanval** — ook bekend als sniffing- of snoopingaanval, is een inval waarbij de hackers proberen informatie te onderscheppen die een voertuig via een netwerk verstuurt.
- **Black-holeaanval** — is een veel voorkomende aanval waarbij de hacker zich tussen de zender en de ontvanger plaatst en stopt met het doorsturen van berichten. Door een gat te slaan is de ontvanger beter in staat om berichten te ontvangen en kan hij zijn realtime werking verhinderen. Bij een *grey-holeaanval* stuurt de aanvaller slechts een gedeelte van de berichten door, hetgeen de kansen om gevat te worden verkleint.
- **Replay-aanval** — is een soort black-holeaanval maar in plaats van berichten te droppen, manipuleert de aanvaller het bericht om de ontvanger aan te vallen.
- **DoS-aanvallen (Denial of Service)** — wanneer een hacker het doelwit overspoelt met uiterst prioritaire berichten die voorkomen dat de legitieme gebruiker nog andere berichten kan ontvangen of verwerken.
- **Bus-offaanval** — is een aanval van het type DoS waarbij de indringer voortdurend bits verzendt, zowel in het ID- als in andere velden, hetgeen de teller van de transmissiefouten van de ECU activeert, tot de CAN-bus geen berichten meer kan versturen of ontvangen.
- **Timingaanvallen** — een hacker introduceert een tijdsvertraging en stuurt ze naar andere voertuigen in de omgeving, wat leidt tot incorrecte instructieplanning en nepcongestie. Deze inbraak kan catastrofale gevolgen hebben voor transportnetwerken die op realtime applicaties gebaseerd zijn.
- **Sybilaanval** — wanneer de aanvaller verschillende identiteiten genereert en elke identiteit gebruikt om verschillende berichten te sturen naar andere voertuigen, voetgangers en infrastructuur. De

bedoeling van Sybilaanvallen is om andere voertuigen, voetgangers en infrastructuur te misleiden opdat ze de foute actie zouden ondernemen.

5.2 Aanvalsoppervlakken

In het geval van geconnecteerde auto's ligt de focus op de aanvallen vanop afstand. De aanvalsoppervlakken verwijzen in deze context naar de potentieel kwetsbare toegangspunten (voor aanvalsvectoren) waar een onbevoegde gebruiker kan proberen gegevens in het voertuig binnen te brengen, eruit te halen of te manipuleren om zich ongeoorloofd toegang te verschaffen.

- **Voertuigtelematica:** telematicadiensten stellen het voertuig in staat operationele gegevens te verzamelen en door te sturen naar de 'head end' telematicasystemen die onder controle staan van een Telematics Service Provider (TSP), alsook om gegevens te ontvangen vanuit de systemen van de constructeur of andere dienstverlenende derden. De on-board systemen die hiervoor instaan zijn het OBD-apparaat (On-Board diagnostics) en de TGU (telematics gateway unit).

  De meerderheid van de informatie die door het voertuig ingezameld en verstuurd wordt bestaat in normale omstandigheden uit informatie over de locatie, tijdstempels en gegevens die de status en de omstandigheden van de kritieke onderdelen van het voertuig weergeven. Die gegevens worden gebruikt om het periodieke onderhoud te plannen en bij garantieaanspraken of om reële prestatiegegevens te verzamelen en naderhand te analyseren.

  Data die naar het voertuig verstuurd worden zijn onder meer verkeersinformatie en navigatiegegevens, informatie over onderhoudsbeurten en zelfs over-the-air software-upgrades.

  Sommige leveranciers van telematicadiensten bieden de eigenaar van het voertuig de mogelijkheid om vanaf een afstand via een app op zijn telefoon met het voertuig te interageren. Zo kan de eigenaar de klimaat regeling al voor het vertrek inschakelen, kaart- en navigatie-informatie opladen naar het IVI-systeem, het voertuig lokaliseren met de gps, de toeter en de lichten bedienen of zelfs vanop afstand het portier openen.

  De telematicasystemen aan boord zijn via de kernnetwerken van het voertuig verbonden met zijn kritieke subsystemen. Ze bestaan uit tal van kleinere elektronische systemen. De draadloze communicatie verloopt over xG-netwerken. Ze wordt geleverd via een cellulaire modem en een simkaart, of door een eigen machine-to-machine module met de modem- en simkaarttechnologie geïntegreerd in één toestel. Sommige van de onderliggende telecommunicatietechnologieën die voor de telematicadiensten worden gebruikt, zoals xG, zijn inherent onveilig door hun ondersteuning voor plaintext-gegevenstransmissie of zwakke encryptie en het ontbreken van wederzijdse authenticatie tussen het mobiele apparaat en het cellulaire basisstation.
- **SMS API:** soms worden sms-berichten gebruikt als backupkanaal voor de informatie-uitwisseling. Die kunnen evenwel onderschept en gedecodeerd worden om aan vertrouwelijke informatie te komen. Hackers kunnen ook knoeien met de sms-commando's (vervangen of veranderen van het versturende mobiele nummer) en rechtstreekse commando's naar het toestel sturen.
- **Web Interface en mobiele API's:** hackers openen accounts op een webinterface en gebruiken daarvoor parameters zoals SIM-nummers. Door een webapplicatie te gebruiken kan de aanvaller vervolgens toegang krijgen tot nog meer inloggegevens.
- **Mobiele apps:** hackers vallen kwetsbare plekken aan in mobiele apps die toegang verschaffen tot autosystemen als de radio. De aanvaller kan dan bestanden laten draaien op de multimedia-apparatuur.

- **Entertainmentsysteem:** hackers kunnen multimediabestanden aanmaken die de code op het systeem veranderen. Dat opent mogelijkheden om gebruik te maken van het systeem en zelfs andere delen van geconnecteerde voertuigen te bespieden.

- **Firmware-upgrades:** tijdens firmware-upgrades mag het systeem geen externe gegevens accepteren. Als het daarin faalt kunnen backdoor-aanvallen het gevolg zijn, waardoor de auto gelinkt wordt aan het systeem van de aanvaller.

- **Wireless Media:** hackers kunnen kwetsbare plekken aanvallen in draadloze kanalen zoals Bluetooth of wifi, die de beheerdersbevoegdheden kunnen omzeilen.

- **Externe sensoren:** hackers kunnen knoeien met de externe sensoren en het voertuig verplichten om ongewenste acties te ondernemen.

- **Wireless Key Entry:** hackers maken gebruik van de toegang voor de draadloze sleutel via een proxy-bridge tussen de sleutel en de auto, die ze daarna naar believen kunnen openen of sluiten.
- **Toegang tot een extern apparaat via de OBD II-poort:** kan hackers toegang bieden tot de interne systemen van het voertuig.

- **Aanvallen op de Cloud-dienstverlening van de autoleverancier:** stellen de hacker potentieel in staat om met één aanval veel auto's te bereiken. We kunnen verwijzen naar de aanval op het Tesla-wagenpark in 2020.

- **Het monitoringsysteem voor de bandendruk:** banden bevatten soms druksensoren die realtime gegevens doorsturen naar een ECU. Dat stelt aanvallers in staat om nepberichten over platte banden te versturen en rijdende voertuigen tot stilstand te brengen. Bij een modern voertuig dat zogezegd een platte band heeft, kan ook het starten worden verhinderd.

5.3 Aanvalsvectoren

Aanvallers kunnen gebruik maken van de aanvalsoppervlakken via uiteenlopende aanvalsvectoren, methoden om die punten uit te buiten.

Servers: de meeste kwaadwillige incidenten maken gebruik van back-endservers. Het gaat om een brede waaier aan incidenten, met onder meer bedienen van telematica en controleservers, smart mobility-toepassingen en inbreken in webservers, zoals de website van een OEM, of gegevensbanken met data over voertuigen, klanten, codes en chauffeurs. Serveraanvallen zijn vaak gericht op kwetsbare plekken en misconfiguraties met TSP's, die voertuigen gegevens laten uitwisselen met servers via een cellulair netwerk. Die servers slaan de data op die van de verschillende voertuigen komen en verwerken aanvragen voor afstandsopdrachten afkomstig van de smartphone-app, zoals het starten van de motor of het afsluiten van de wagen. Servers vormen ook een favoriete vector voor criminelen die gebruik maken van ransomware.

Remote keyless entry: vier tendensen kenmerken dit type aanval dat almaar vaker voorkomt. Eén is het programmeren van sleutels om de diagnoseconnector te manipuleren en dure auto's te stelen. Die vector komt vaak voor in Europa, waar privacywetten voorschrijven dat de gegevens die via de OBD-connector beschikbaar zijn niet gecodeerd mogen worden. Keyless jamming is een andere techniek waarbij het signaal om de auto af te sluiten geblokkeerd wordt. Spoofing omvat het stelen van de cryptografische sleutel van voertuigen. Tot slot zijn er de relay hacks, waarbij de criminelen een relay box gebruiken om het signaal van een sleutelhanger op te vangen en zo een voertuig te openen.

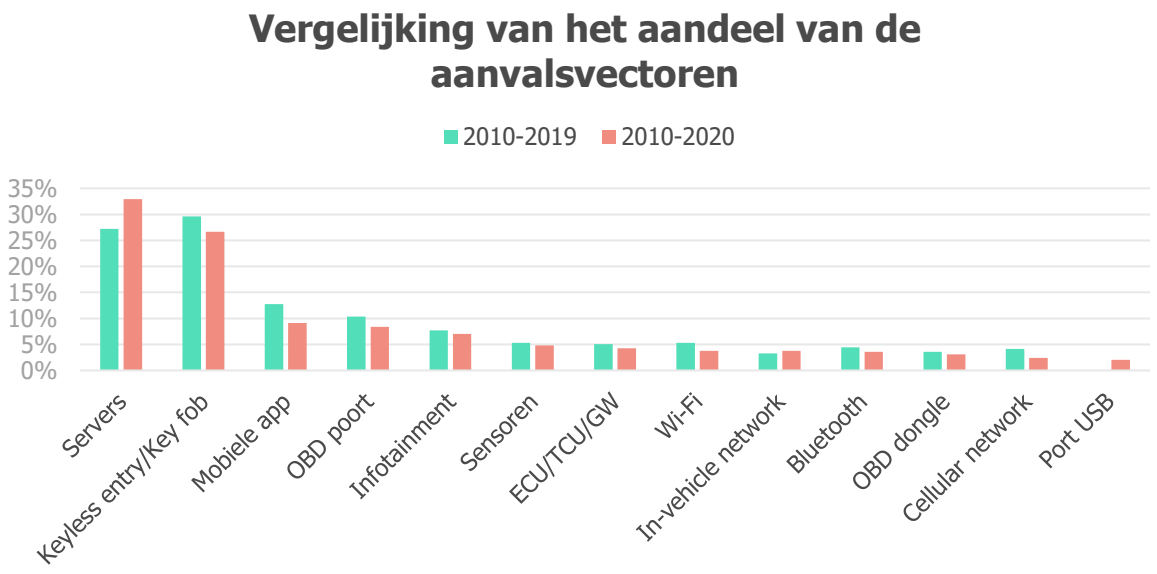
OBD-poort: OBD-systemen geven de eigenaar en de onderhoudsmecanicien toegang tot de status van de subsystemen van een voertuig. Voor een aanval op de OBD-poort moet de hacker zich oorspronkelijk fysiek toegang tot de auto zelf verschaft hebben, wat het wel uitdagender maakt. Soms heeft een OBD-poort echter een dongle/transceiver via bluetooth, wifi of cellulair voor de diagnoses of voor een vlotte toegang, of vooraf geplaatst door de hacker. Dat kan resulteren in autodiefstal of het inbrengen van kwaadwillige CAN-

busberichten om het gedrag van het autosysteem te manipuleren, bijvoorbeeld door het gebruik van een signaalstoorzender die belet dat de auto op slot gaat. Veel aanvallen via de OBD-poort worden veroorzaakt door OBD dongles die de hackers rechtstreeks vervaardigd hebben.

Mobile App: OEM's ontwikkelen vaak apps om de autobezitter vanaf een afstand een aantal functies te laten bedienen, of met het oog op toegankelijkheid of gebruiksgemak. Vooreerst kunnen aanvallers inbreken in de app zelf, via reverse-engineering kwetsbare plekken zoeken en die gebruiken om toegang tot de auto te krijgen. De telefoon zelf bemachtigen maakt het voor de crimineel natuurlijk nog gemakkelijker om de auto of zijn voertuiggegevens te stelen. Daarnaast zijn niet alle apps wat ze lijken. Ze kunnen nep en kwaadwillig zijn. Aanvallers gebruiken die om wachtwoorden en accounts te onderscheppen en daarmee de controle over de voertuigen over te nemen. Tot slot zijn er nog man-in-the-middle-aanvallen waarbij mobiele apps persoonsgegevens en voertuigcontroles aan de aanvallers uitleveren. Een derde partij misbruikt of wijzigt de legitieme verbinding van de gebruiker, wifi in dit geval.

Infotainment: het meest gebruikelijke toegangspunt om in de IVI-systemen te komen is door het afspelen op de multimediasystemen van speciaal bewerkte mediabestanden. Dat kan gebeuren met audio via bluetooth, wifi of Android auto. Ook de USB-poort is een mogelijkheid als door de gebruiker of via social engineering een USB-to-wifi-adapter geconnecteerd is.

De onderstaande grafiek vergelijkt het aandeel van de malwarevectoren in de periode 2010-2019 en 2010-2020. Servers, 'sleutelloos' en mobiel zijn nog altijd de meest voorkomende vectoren.[2]



[2] Gebaseerd op Upstream Security: Global Automotive Cybersecurity Report 2021.

5.4 Gevolgen en scenario's

Rolljamaanval:

Autosleutels gebruiken een radiofrequentie om de auto te openen. Om aanvallers te beletten dat 'ontgrendelbericht' zomaar op te vangen gebruiken autoconstructeurs een systeem van zogeheten 'rolling codes' waarbij de sleutel de code volgt binnen een opeenvolging van codes verbonden aan de auto, zodanig dat aanvallers, althans in theorie, de volgende code niet kunnen raden.

Toch heeft ook 'rolljam' zijn kwetsbare plekken. Een rolljamaanval is bedoeld om verstopt te worden op, of bij het beoogde voertuig of in de garage, waar het wachten is op een argeloos slachtoffer dat zijn sleutel met radiobereik gebruikt. Het slachtoffer zal alleen merken dat de sleutelhanger het niet deed bij de eerste poging, is zich van geen kwaad bewust en probeert het nog eens. Dit keer is de druk op de knop wel succesvol en de auto gaat open. De aanvaller kan op ieder moment terugkeren om het toestelletje op te halen.

In de praktijk werkt dit als volgt: er wordt gewacht tot de eigenaar op de knop drukt om te openen. De aanvaller verstuurt een blokkeersignaal waardoor de auto de eerste opdracht om te openen niet ontvangt. De aanvaller registreert de eerste opdracht om te openen, terwijl hij die blokkeert voor de ontvanger in de auto. Dat kan doordat de auto een breder bereik aftast dan het bereik waarbinnen de sleutel uitzendt. Het blokkeersignaal klinkt dus 'harder' dan de autosleutel.

De eigenaar stuurt nu het tweede signaal om te openen dat op zijn beurt geblokkeerd en opgenomen wordt. De aanvaller verstuurt nu meteen het opgenomen eerste signaal, maar de eigenaar is in de overtuiging dat hij de auto opende met het tweede signaal. Dat tweede signaal wordt ondertussen bewaard om er later de auto mee te openen.

Impact: als de aanvaller een succesvolle rolljamaanval plaatst kan hij, afhankelijk van het model, de portieren openen (althans één keer) en toegang krijgen tot de cockpit. Behalve het probleem van de diefstal zal de aanvaller de auto wellicht niet kunnen starten omdat de sleutels ontbreken en de elektronica uitgeschakeld is. Dit kan echter wel een goed moment zijn om stiekem kwaadwillige elektronica, zoals een draadloze OBD II dongle aan te koppelen of in te pluggen. Die kan dan later gebruikt worden om de controle over de auto over te nemen, wanneer de gebruiker hem inschakelt.

OBD II Dongle-aanvallen:

De OBD2-poort wordt gebruikt voor on-board diagnose via het CAN-protocol, een seriële-busstandaard voor broadcastconnectie met ECU's, wat wil zeggen dat er geen centrale computer is. Als een ECU een bericht stuurt zal elke andere ECU op de bus die ontvangen om er op te reageren of het te negeren. Het apparaat dat de motor controleert stuurt bijvoorbeeld continu een CAN-bericht met de snelheid (in RPM). Normaal wordt de OBD II-poort alleen gebruikt om diagnose-info uit te lezen, maar met wat speciale apparatuur en elektronica kan ze ook CAN-berichten in het netwerk inbrengen gericht op de ECU's. En om de stap te kunnen zetten naar draadloze aanvallen kan ook een kwaadwillige draadloze dongle stiekem in de OBD2-poort geplugd worden.

Impact: de OBD II-poort maakt een rechtstreekse connectie mogelijk met het CAN-netwerk. Dat maakt het mogelijk om zo goed als elk subsysteem in een voertuig te bevragen en te wijzigen. Wie slechte bedoelingen heeft kan de poort gebruiken om de veiligheid of de beveiliging van het voertuig aan te tasten. Door nieuwe sleutels te programmeren, kunnen de alarmsystemen bijvoorbeeld geneutraliseerd worden, of gewijzigde kalibratiegegevens opgeladen naar de Engine Control Module (ECM) of nog airbags en andere veiligheidssystemen uitgeschakeld.

TPMS-aanval:

De TPMS (Trusted Platform Module System) in de band stuurt via radiogolven informatie naar de ECU van het voertuig. Daarbij monitort hij voortdurend de bandendruk om de ECU in staat te stellen een boodschap naar het dashboard te sturen zodra de druk buiten de opgegeven waarden valt. Van die systemen is bekend dat ze zonder echte beveiliging werden ingevoerd. Een eventuele passieve aanval kan de aanvallers in staat stellen om de beweging en de locatie van het voertuig te volgen, gebruik makend van mobiele en langs de weg gelegen stations, aangezien TPMS-signalen opgevangen kunnen worden tot op 40 meter van het voertuig. Anderzijds kan het gebrek aan encryptie van de TPMS-signalen een actieve aanval mogelijk maken, omdat de ECU alle informatie vertrouwt die van de sensoren van het voertuig komt. Daardoor is het mogelijk om draadloos gemanipuleerde signalen te injecteren die de ECU misleiden om valse bandendrukwaarden weer te geven. Bij bepaalde moderne auto's kan het zelfs lukken om de auto te doen stoppen of de motor het starten te laten weigeren.

Impact: met Software Defined Radios (SDR) kan de radio geanalyseerd en gebruikt worden. Met TPMS is het mogelijk om een actieve aanval uit te voeren, gebruik makend van de SDR en daarbij het voertuig te laten denken dat de TPMS waarschuwen voor een te lage bandenspanning, terwijl alle banden in werkelijkheid correct opgepompt zijn. Dit kan een wezenlijk risico inhouden voor de inzittenden van het voertuig, als zich bijvoorbeeld een belangrijke persoon in de wagen bevindt en het aantal haltes op het traject tot het minimum beperkt moet worden om blootstelling aan een aanval te voorkomen. Bovendien creëert in de context van transportinfrastructuur het bezwijken van één systeem in de keten ook een risico voor andere voertuigen of systemen.

Infotainmentaanval:

Infotainment biedt de gebruiker toegang tot telefonie, audio, video, satellietnavigatie en live verkeersinformatie en soms zelfs internetconnectiviteit en toegang tot diensten. Het resultaat is dat er tal van bedrade en draadloze interfaces met het systeem communiceren, waarvan een aantal toegankelijk is voor de inzittenden van het voertuig, terwijl sommige vanaf een afstand benaderd kunnen worden. Het gaat om radio, Bluetooth, wifi en andere geconnecteerde diensten. We kunnen proberen om die interfaces en poorten te onderzoeken op zwakke plekken die kunnen leiden tot gegevensmanipulatie en zelfs privilege-escalatie in het systeem. Omdat die infotainmentsystemen onderling verschillen zal een algemene verkenning van een bepaald systeem nodig zijn om daarna de zwakke punten te kunnen evalueren.

Impact: individuele IVI-systeemcomponenten kunnen ontworpen en geproduceerd zijn door ondernemingen van uiteenlopende derden, die wellicht verschillende kwaliteitsnormen hanteren wat betreft de ontwikkeling van veilige code. Het resultaat is dat de kans op kwetsbare plekken in de software vrij groot is, hetgeen een risico inhoudt voor de veiligheid van het voertuig. Omdat een logisch netwerkpad van buiten en draadloos naar het interne CAN-netwerk leidt, zal in theorie elke kwetsbare plek die gebruikt kan worden om de controle over het IVI-systeem over te nemen en frames naar het interne CAN-netwerk te sturen, ernstige gevolgen kunnen hebben. Dat kan ook als de gebruiker naar onveilige links navigeert die het systeem proberen te infecteren en manipuleren. Als de aanvaller tot slot toegang tot en controle over het IVI-systeem kan krijgen, kan hij ook zijwaarts bewegen om te connecteren met een smartphone van de gebruiker die met het IVI-systeem geconnecteerd is. Dit biedt op zijn beurt een aanvalspad naar het mobiele apparaat van de gebruiker.

5.5 Toegepaste aanvalsscenario's

In dit hoofdstuk geven we de aanvalsscenario's zoals ze voorbereid, uitgevoerd en beschreven werden door de stagiair van Howest University. In de video zijn opnames te zien van de uitgevoerde aanvallen.

5.5.1 Rolljamaanval

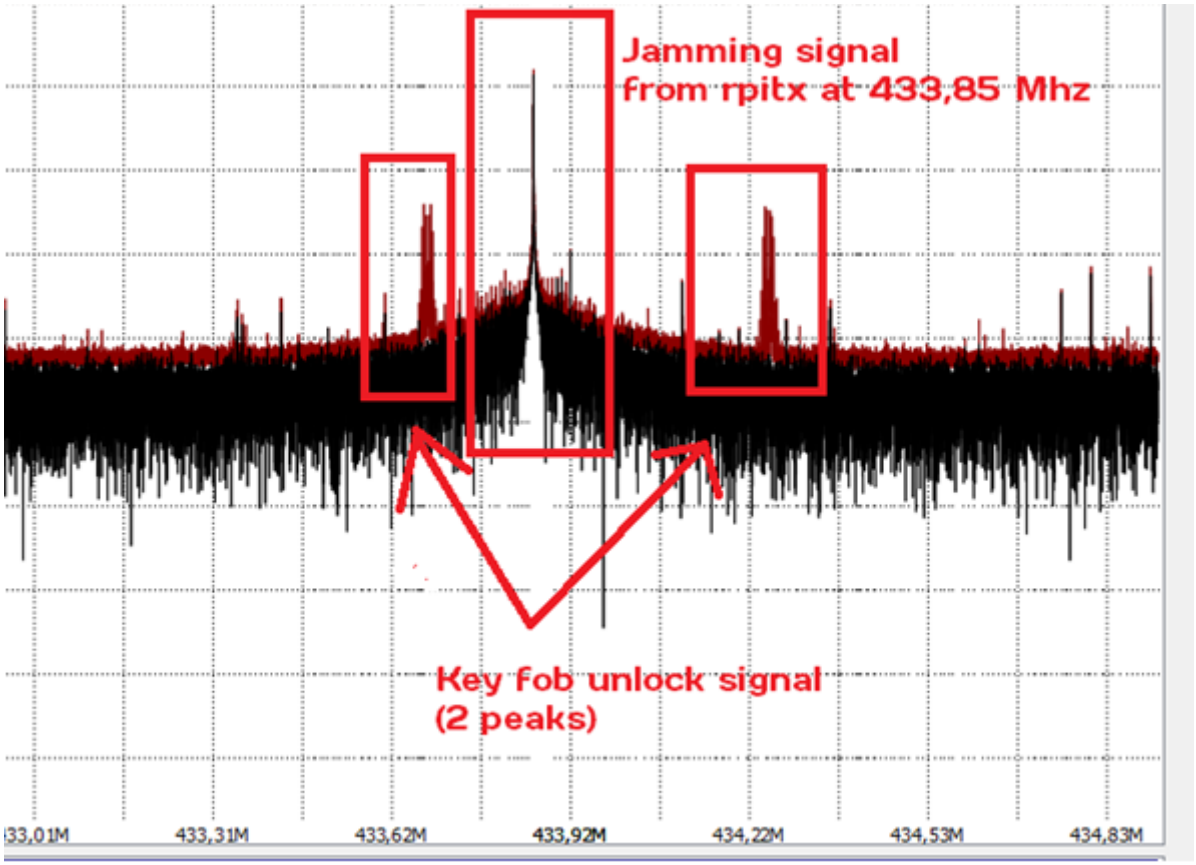
Bij de aanval waarbij ik de deur kan openen door op een radiofrequentie een niet-gebruikt signaal daartoe op te vangen, moest ik tijdens het opnemen en luisteren naar het ontgrendelsignaal het signaal blokkeren. Ik gebruikte daarvoor een Raspberry Pi3 B+, een kleine singleboardcomputer die populair is vanwege zijn lage kostprijs van rond de $35 en zijn modulaire en open ontwerp. Daarbij komen nog de open source software RpiTX voor radiofrequenties en een draad op een van de contacten die dienst doet als antenne.



Om vervolgens het signaal te beluisteren en op te nemen, heb ik gebruikgemaakt van een HackRF One. Dat is een breedband SDR (software defined radio) van $330 een half-duplex transceiver, wat inhoudt dat hij radiosignalen uitzendt en ontvangt, maar niet tegelijkertijd. Het gevolg is dat we zeer snel moeten ontvangen en ons signaal versturen. Om die reden gebruiken we de Raspberry Pi, in combinatie met de HackRF One. Het is ook een handig instrument voor professionals in beveiliging, omdat het werkt in een frequentiebereik van 1MHz tot 6GHz, terwijl de hardware ook een open source project is.



Bij de rolljamaanval proberen we in wezen het 'rolling code'-systeem te omzeilen waarbij de sleutelhanger en de wagen beide een opeenvolging van codes afgaan om te controleren op authenticiteit. We doen een poging om die maatregelen tegen te gaan. Omdat de auto radiofrequentiesignalen ontvangt, heeft hij een ontvangstvenster, een frequentiebereik. Dat wil zeggen dat we een frequentie kunnen blokkeren in de buurt van maar niet boven op de frequentie van de auto. Als we direct op het ontgrendelsignaal zouden blokkeren zouden we niet in staat zijn om het op te nemen. Bij het testen moest ik eerst op zoek naar de correcte radiofrequentie die de sleutelhanger gebruikt. Door te luisteren en spectrumanalyzers in te zetten kon ik de frequentie lokaliseren die zich rond de 434MHz bevond. Ik werd echter verrast door iets dat ik niet verwacht had.



Tijdens het gebruik van de sleutelhanger om de deur te ontgrendelen kregen we op het spectrogram niet één maar twee pieken te zien! Op dat moment was ik er vrij zeker van dat dit nog een mechanisme en een maatregel zou zijn om aanvallers die het met rolljamaanvallen willen proberen tegen te gaan en een stap voor te blijven. Ik kon niet uitmaken hoe dit precies in zijn werk gaat, maar ik neem aan dat een algoritme of mathematische functie gebruikt wordt om het signaal te decoderen uit de combinatie van pieken. Ongeveer al mijn pogingen om te blokkeren bleven zonder gevolg. Het was ongelofelijk om te beseffen hoe mijn aanval tegen een tegenmaatregel alweer op een nieuwe tegenmaatregel stootte die daar nog eens bovenop kwam. Dit illustreert perfect het kat-en-muisspel dat hackers en beveiligingsprofessionals spelen om elkaar altijd weer een stap voor te blijven.

5.5.2 Infotainmentaanval

In de volgende aanval koos ik voor het infotainmentsysteem en probeerde daar zwakke plekken in aan te treffen. Over het algemeen werken die systemen nogal als een gewone computer of een gewoon besturingssysteem. De meeste draaien ook op Linux of Android.

Omdat de focus op draadloze aanvallen ligt, startte ik meteen bij de verkenningsfase. Daarbij proberen we een maximum aan informatie over een doelsysteem te verzamelen. Ik keek uit naar open interfaces en onderzocht het apparaat om uit te zoeken op welk besturingssysteem het infotainment draaide.

Het infotainmentsysteem gebruikt wifi voor zijn communicatie met de buitenwereld en met andere apparaten. Dat betekent dat we met een ander wifi-compatibel toestel, zoals een wifi-adapter naar het apparaat kunnen luisteren en ermee communiceren. Ik besloot ook om aan een adapter te komen met monitormodus. Dat houdt in dat hij alle wifipakketten accepteert die doorgestuurd worden, terwijl normale adapters vaak alleen data accepteren die op hen gericht zijn en de andere gegevens negeren. Met die kennis in het achterhoofd koos ik de wifi-adapter met monitoringmodus TP-LINK TL-WN722N van ongeveer $15.



Ook hier werd ik weer verrast. Na zorgvuldig onderzoek van het systeem bleek voor infotainment Alpine Linux gebruikt te worden, een veiligheidsgerichte Linux-distributie. Standaard laat Alpine Linux geen interfaces open naar de buitenwereld, wat mij machteloos achterliet met het oog op de volgende stappen. Het accepteert daarmee alleen signalen die het verwacht te ontvangen.

We moeten erop wijzen dat hacken niet onmogelijk is, maar datgene waarvan de constructeurs vreesden dat het voor aanvallers het centrale punt zou zijn is kennelijk goed beveiligd. Zelfs als ik in staat was geweest om het systeem te kraken, had ik bovendien verdere aanvallen moeten lanceren en rondjes draaien om in de kritieke elektronica van de auto te geraken. Daarom besloot ik het erbij te laten en door te gaan met de resterende twee.

5.5.3 OBD II-aanval

Een OBD II-aanval berust op een connectie die de aanvaller heeft met de OBD-poort. Om dat uit te breiden tot een draadloze aanval kan een draadloze dongle toegevoegd worden die rechtstreeks met de CAN-bus communiceert terwijl hij vanaf een afstand aangestuurd wordt. Er zijn uiteenlopende manier om zo'n dongle te plaatsen. De chauffeur kan hem bijvoorbeeld installeren om de status van de auto-elektronica op zijn smartphone na te gaan. Hij kan ook gecombineerd worden met de rolljamaanval om de deur te ontgrendelen en geplaatst worden buiten medeweten van de chauffeur. Aangezien de OBD-poort voor de chauffeur behoorlijk goed verborgen ligt is ze moeilijk te zien.

Voor deze aanval was de macchina P1 mijn tool. Dat is een volwaardige Linux-computer met een OBD II-connector, die CAN-berichten kan lezen en schrijven. Daarbij heeft hij een PocketBeagle voor de wifi-functies. De prijs bedraagt zo'n $150.



Nadat we er de beagleboard Debian Linux-distributie op geïnstalleerd hadden, konden we ermee connecteren. We kunnen de tool dan in de OBD II-poort van de auto plaatsen en wachten tot alle blauwe lichtjes branden, wat betekent dat de bootsequens succesvol was. We kunnen nu de SSH terminal openen en commando's schrijven.

Doorgaans zal de auto twee virtuele CAN-interfaces hebben, can0 en can1. De beide gebruiken een bepaalde baudfrequentie en aangezien elk auto verschillend is moeten we uitzoeken welke dat precies is. Na wat gissen en missen kon ik erachter komen (voor een Volvo V40) dat de baudfrequentie voor can0 500K bedraagt en die voor can1 125K. We stelden daarop de juiste baudfrequentie in om te luisteren en te lezen wat zich binnen in de CAN-bus afspeelt.

```
debian@beaglebone: ~
debian@beaglebone:~$ candump -cae can1,0:0,#FFFFFFFF
  can1  050   [8]  A8 00 00 00 00 53 50 88   '.....SP.'
  can1  2C0   [8]  A0 00 00 00 09 02 64 90   '......d.'
  can1  504   [8]  04 01 00 00 03 00 00 00   '........'
  can1  0F0   [8]  2F 00 00 35 0A 02 64 90   '/..5..d.'
  can1  505   [8]  05 01 00 00 03 00 00 00   '........'
  can1  050   [8]  A8 00 00 00 00 53 50 88   '.....SP.'
  can1  020   [8]  00 80 31 B0 2F 22 E2 C0   '..1./"..'
  can1  025   [8]  30 00 00 00 04 00 00 00   '0.......'
  can1  501   [8]  01 01 00 00 00 00 00 00   '........'
  can1  060   [8]  40 04 00 7F 00 00 00 00   '@.......'
  can1  080   [8]  81 D1 00 00 00 00 00 12   '........'
  can1  0F0   [8]  2F 00 00 35 0A 02 64 90   '/..5..d.'
  can1  07A   [8]  0C 00 00 60 00 80 80 00   '...`....'
  can1  050   [8]  A8 00 00 00 00 51 D0 88   '.....Q..'
  can1  0D5   [8]  60 00 00 01 02 03 00 00   '`.......'
  can1  010   [8]  00 00 00 00 08 00 04 00   '........'
  can1  0B0   [8]  00 00 00 00 00 00 00 00   '........'
  can1  2D4   [8]  00 00 00 00 00 00 00 00   '........'
  can1  020   [8]  00 00 31 B0 2F 22 E2 C0   '..1./"..'
  can1  0D0   [8]  00 00 00 00 00 00 00 00   '........'
  can1  104   [8]  04 00 40 00 00 00 00 01   '..@.....'
```

We werden onmiddellijk overspoeld door duizenden CAN-berichten over de CAN-bus en waarvan we voor een groot deel niet weten wat ze betekenen. Dat wil zeggen dat we heel wat tijd gespendeerd hebben aan reverse engineering en decoderen van de inhoud door een bepaalde actie zoals het openen van de deur door te drukken en de berichten te bekijken en te bewaren, om ze dan te vergelijken en uit te zoeken welk bericht wat betekent.

Nadat ik door heel wat CAN-berichten gegaan was kon ik uitmaken dat één enkel bericht niet echt voor iets stond, wel ruwweg een opeenvolging van berichten. We kunnen die opeenvolging dan nemen en terugsturen naar de CAN-bus, om door andere elektronica opgepikt te worden. Op die manier was ik in staat om een ontgrendelsequens te faken en de andere elektronica in het voertuig in de waan te laten dat de deur open is en dat zelfs visueel weer te geven op het dashboard.



Ik merkte echter ook op dat die berichten een zeker eenmalig of tijdsgebaseerd mechanisme gebruiken om te vermijden dat het bericht voortdurend verstuurd wordt. Dat wil zeggen dat zodra een sequens verstuurd is, deze meestal geen tweede keer meer zal werken. Om die reden moeten we een nieuw signaal krijgen van de auto door een actie door te drukken of eventueel een auto te simuleren met dezelfde parameters. We kunnen dus niet alleen afluisteren en elke beweging en verandering van de auto volgen, maar nu ook zelf vervaardigde berichtsequensen inbrengen om de auto en zijn kritieke elektronica beet te nemen en mogelijk gevaarlijke commando's te doen volgen.

5.5.4 TPMS-aanval

De meeste moderne wagens hebben op de banden een stel sensoren die de druk meten en die informatie naar de 'cockpit' en andere elektronica sturen. Aangezien het wiel een draaiend onderdeel is, kan hier niet anders dan met een radiofrequentie gewerkt worden om de waarden door te geven.

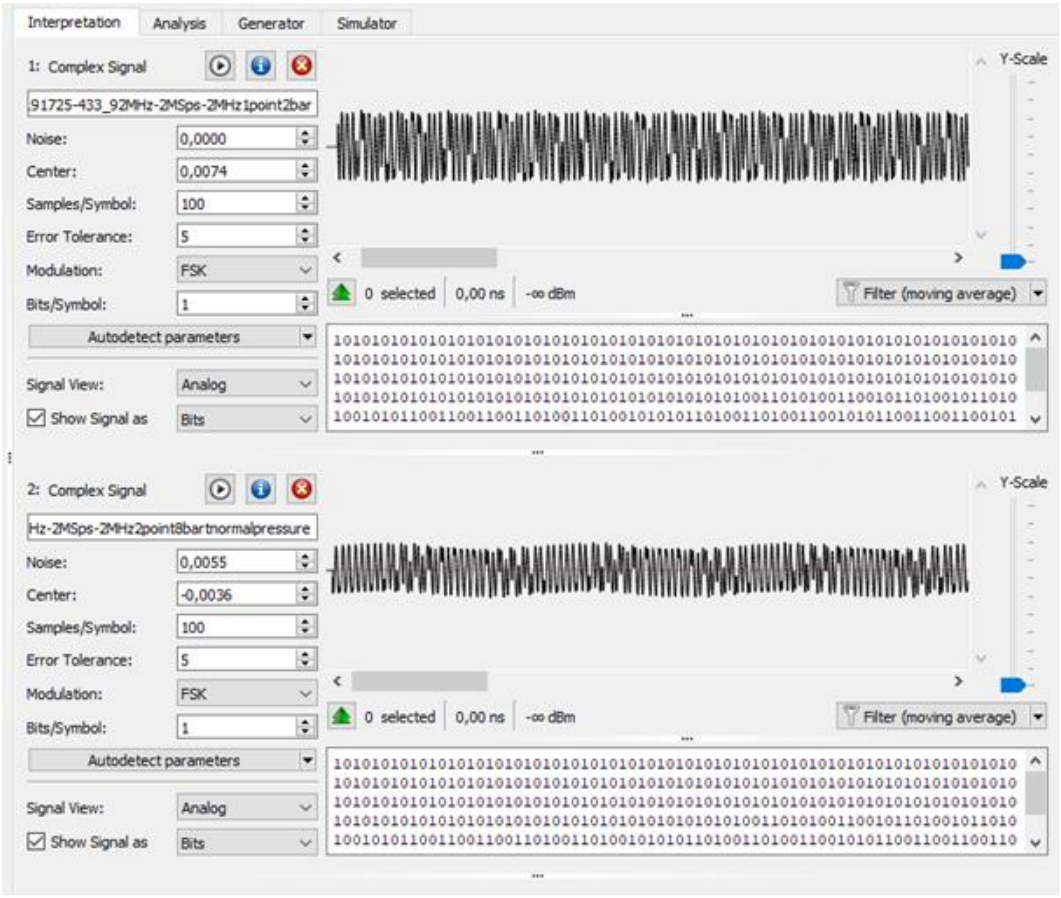
En daar komt de TPMS-aanval in het vizier. We zullen proberen om een nepsignaal door te sturen met een nepwaarde voor de bandendruk, onder het toegestane minimum voor veilig rijden, waardoor de auto ervan overtuigd is dat een band plots leeggelopen is, wat echter niet het geval is. Hier heb ik gebruikgemaakt van de eerder beschreven HackRF One, samen met een Jansite TPMS-systeem.



Om te beginnen moeten we uitvissen op welke frequentie die toestellen werken. Met de Hackrf One en een spectrumanalyzer wou ik wachten tot een signaal doorgestuurd zou worden. Dat gebeurde aanvankelijk niet, hoe vreemd ook. Je zou verwachten dat periodiek een signaal wordt doorgestuurd, maar dat is blijkbaar verkeerd gedacht. De meeste tijd staat de auto immers stil en is er geen enkele behoefte om voortdurend waarden door te sturen.

Op de manier waarop de sensoren ontworpen zijn sturen ze enkel een signaal uit bij een verandering van waarde. Omdat ik de banden van de auto niet wou laten leeglopen, heb ik ze gekoppeld aan een fiets om gemakkelijk de banden te kunnen oppompen en aflaten en het uitzenden van een signaal uit te lokken. Ook hier was de gebruikte radiofrequentie 434Mhz.

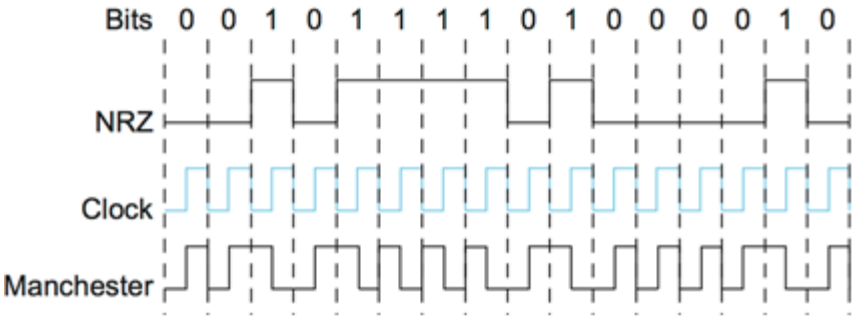
Ik heb twee keer het triggersignaal van de sensoren opgenomen, één keer bij normale druk, 2,8 bar en een tweede keer met de 'plattebandwaarde' van 1,2 bar.



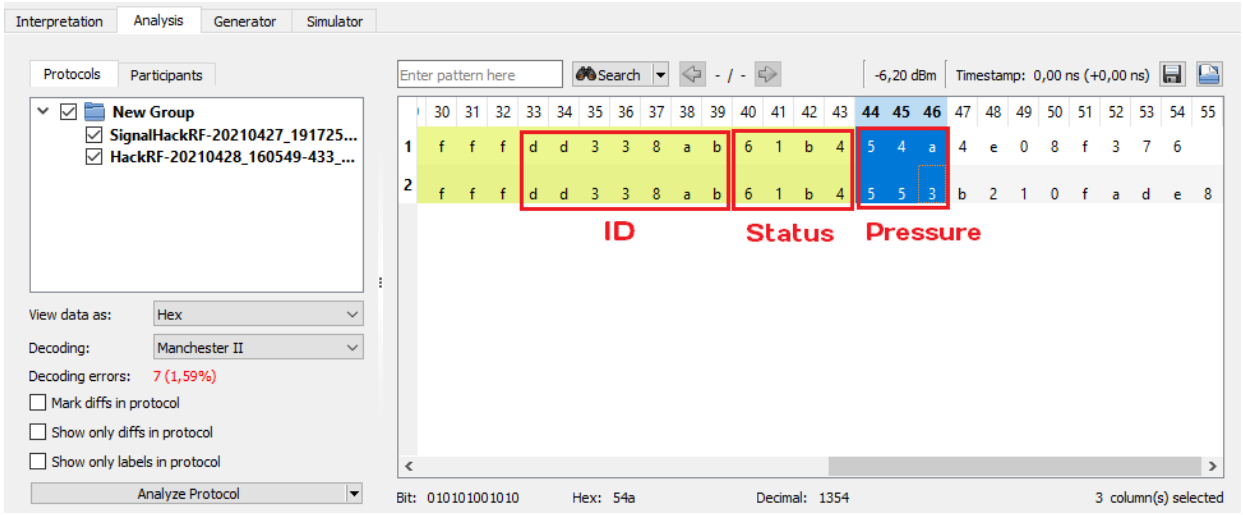
Aangezien het signaal een radiofrequentie gebruikt, moeten we eerst omzetten naar binair. We krijgen dan iets in de aard van:

10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
10101010101010101010101010101010101010101010011010100110010110100101101010010101100110011001101001101001010101101
01101001100101011001100110010110011001011001011010100101010101100101011010101001011010011010100110100100000000

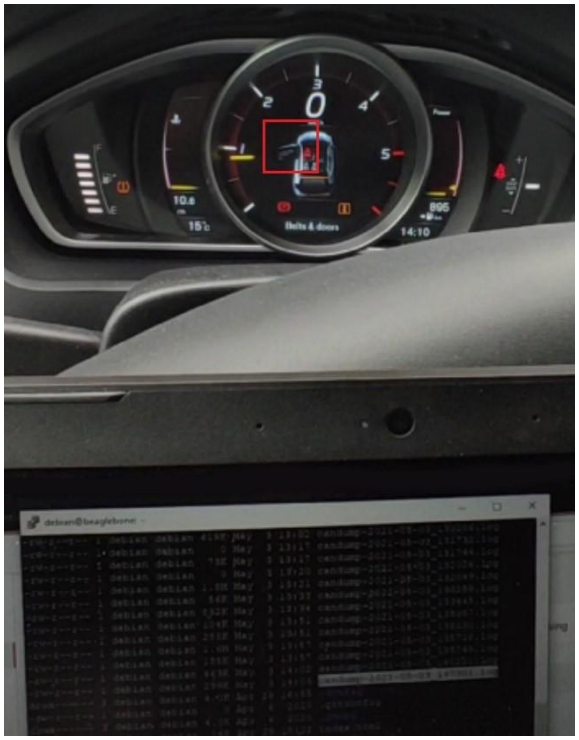
Nu volgt het gedeelte waarin we op zoek moeten naar het correct coderen van deze gegevens. Na even aandachtig kijken, merkten wat we vaak 2 keer een 0 of 2 keer een 1 zien, maar nooit 3 keren een 0 of een 1. Dit wijst heel waarschijnlijk op Manchestercode. Die wordt gebruikt voor zelfkloksignalen zonder DC-componenten.



Nu we weten dat we met Manchestercode te maken hebben, kunnen we de waarden decoderen naar hexadecimaal. In die vorm kunnen we gaan ontleden en proberen uit te zoeken hoe de header er zou kunnen uitzien. Om hier gemakkelijker aan reverse engineering te doen kunnen we twee signalen opnemen, met slechts een minimale wijziging, zoals een drukafname van slechts 0,1 bar en de signalen vergelijken. De ID van het TPMS-systeem zal dezelfde blijven (elk TPMS heeft een eigen unieke ID, om te vermijden dat de auto ernaast jouw waarden toegestuurd krijgt). Daarna volgden we de statusberichten en de feitelijk geregistreerde drukwaarden. Uit die berichten kunnen nuttige data gehaald worden om te analyseren en om de signalen na te maken waarmee we het systeem om de tuin geleid hebben.



Het gevaar hier bestaat erin dat we een voertuig kunnen traceren op basis van zijn unieke TPMS ID, via radiofrequenties, vanaf een relatief middellange afstand, en we kunnen de toestand van de banden en de bandendruk inlezen. Daarbovenop kunnen we ook valse signalen uitsturen als zou de bandendruk te laag zijn, om de auto te doen geloven dat een van de banden plat is, waarna de auto kan stoppen en de motor zelfs kan weigeren om te starten.



Après beaucoup de temps passé par les messages poubelle du CAN, j'ai pu comprendre qu'en fait, il n'y a pas qu'un seul message responsable de quelque chose, mais grosso modo une séquence de messages. On peut ensuite prendre cette séquence et la renvoyer dans le bus CAN pour que d'autres composants électroniques la reprennent. De cette façon, j'ai pu usurper une séquence de déverrouillage des portes, ce qui a poussé tous les autres composants électroniques du véhicule à croire que la porte était bien ouverte, en l'affichant même sur le tableau de bord.

Cependant, j'ai également remarqué que ces messages utilisent un certain mécanisme à usage unique ou basé sur le temps pour empêcher que le message soit envoyé constamment. Cela signifie qu'une fois qu'une séquence est utilisée, elle ne fonctionne plus la plupart du temps. Voilà pourquoi il faut obtenir un nouveau signal de la voiture en forçant une action ou éventuellement une voiture simulée avec les mêmes paramètres. Non seulement on peut lire et suivre chaque mouvement et chaque changement de la voiture, mais maintenant, on peut aussi injecter des séquences de messages conçus pour pousser la voiture et son électronique critique à d'éventuelles commandes dangereuses ultérieures.

6 Bekende pogingen uit het verleden

De analyse van de aanvalspogingen die hieronder beschreven staan is gebeurd op basis van de beschikbare informatie die we haalden uit de pers en de vakbladen, uit presentaties op officiële evenementen en uit academische papers.

ETHISCH (WHITE HAT)					
Naam	**Jaar**	**Interactie met de gebruiker**	**Aanvals-vector**	**Zwak punt**	**Beschrijving**
Chevy Malibu	2011	Ja	Radio	Bluetooth	Na toegang te hebben gekregen tot een 'gateway'-apparaat, (low-speed CAN) konden de aanvallers de remmen manipuleren door het toestel te herprogrammeren tot een high-speed CAN. Ze gebruikten al sync phone.
Chevy Malibu (tweede poging)	2011	Neen	Telematica	Cellulaire verbinding	De aanvallers kozen het telefoonnummer van de eenheid en communiceerden met haar modem, zonder interactie met de chauffeur. De telematicaeenheid was al op een high-speed CAN, zodat ze toegang hadden tot de remmen.
Jeep Cherokee	2015	Neen	Hoofdeenheid	Kwetsbaar punt: toegankelijk via Internet (zwakke wachtwoorden van de constructeur)	Omdat ze hun code konden draaien op de hoofdeenheid waren de aanvallers in staat om een andere processor met toegang tot het CAN-netwerk te herprogrammeren. Op die manier hadden ze stuur, remmen en optrekken onder controle. De cellulaire verbinding van Uconnect geeft ook iedereen die het IP-adres van de auto kent toegang van eender waar.
Tesla S	2016	Ja	CID	Oude versie van de webbrowser	Vereiste fysieke nabijheid door de gebruiker een kwaadwillige website te laten bezoeken of wanneer hij aansloot op een open wifinetwerk. Aanvallers die het zwakke punt kennen herprogrammeren het gatewaytoestel (geconnecteerd met het CID over Ethernet) en konden CAN-berichten sturen en de remmen gebruiken.
Tesla S (tweede poging)	2016	Ja	CID	Oude versie van de webbrowser	Nadat Tesla de code op het gatewaytoestel verbeterd had konden de aanvallers het nog steeds omzeilen en herprogrammeren.
BMW i3	2018	Neen	Telematica	Cellulaire verbinding	De telematica werd via het gatewaytoestel van de high-speed CAN gescheiden, maar de aanvallers waren niet in staat om ze helemaal te omzeilen. Ze konden wel diagnostische CAN-berichten versturen via de gateway naar de high-speed CAN die hen theoretisch in staat stelde om ECU's te herprogrammeren. Wanneer de OBD gebruikt werd via Ethernet of

					Bluetooth-adapter, was het mogelijk om het draadloze signaal van de adapter te hacken. De wagen werd geconnecteerd met het cellulaire bassistation van de aanvallers.
Ford Escape	2013	Aanvaller in het voertuig	n.v.t.	n.v.t.	n.v.t.
Toyota Prius	2013	Aanvaller in het voertuig	n.v.t.	n.v.t.	n.v.t.
Sleutelloos systeem bij Audi, BMW, DS3, Ford, Land Rover, Mercedes-Benz	2019	Ontbrekende gegevens	Sleutelhanger	n.v.t.	Onderzoekers testen zeven verschillende automodellen met een sleutelloze ontgrendel- en starttechnologie en konden in enkele seconden in elk van de zeven inbreken.
Ford Focus	2020	Aanvaller in het voertuig	Hoofdeenheid	Wifi	Met een OBD II-connector en een laptop, konden de onderzoekers de remmen bedienen, de snelheid van de auto veranderen, zich toegang verschaffen tot het infotainment-systeem, en dergelijke meer
Forward-looking Threat Research (FTR) & Politecnico di Milano	2017	Ontbrekende gegevens	CAN	Elk vanaf een afstand bruikbaar zwak punt (bv. infotainment)	Aanval die een toestel uitschakelt (bv., airbag, parkeersensoren, actieve veiligheidssystemen) dat geconnecteerd is met het apparatennetwerk op een manier die voor de huidige geavanceerde veiligheidsmechanismen onzichtbaar is *Merkneutraal.*
Tesla wagenpark	2020	Neen	Telematica	Server-side mechanisme	Een onderzoeker maakte gebruik van een mechanisme aan serverzijde in de Tesla en kreeg toegang tot de 'command and control'-server. Zo kreeg hij controle over elk voertuig in de vloot.

MALAFIDE (BLACK HAT)					
Naam	**Jaar**	**Interactie met de gebruiker**	**Aanvals-vector**	**Zwak punt**	**Beschrijving**
Aanval op wagenpark (Filipijnen, Marokko, India, Zuid-Afrika)	2019	Neen	Traceerapp	Zwakke wachtwoorden in de traceerapp van het wagenpark	Bij sommige auto's is de software (wagenparkbeheer) in staat om vanaf een afstand de motor uit te zetten van voertuigen die stilstaan of trager rijden dan 20 km/u. De hacker ging zo ver niet maar haalde alleen de gegevens op uit de app)
NL & BE trucks	2019	Ontbrekende gegevens	Tachograaf	n.v.t.	Hacken van rijtijd- en snelheidsmeters in trucks

7 Tegenmaatregelen

De beveiligingsarchitectuur van autosystemen die de voorbije jaren tot de norm is uitgegroeid, is een hiërarchische classificatie van 4 niveaus, voorgesteld vanuit beveiligingsstandpunt. Voor elk van die beveiligingsniveaus worden nu al algemene bestaande tegenmaatregelen toegepast.

Beveiliging van niveau 1 (externe communicatieapparatuur)

communiceert met de buitenwereld. Bestaat uit boordapparatuur om te communiceren met draadloze netwerken en met systemen voor communicatie tussen voertuigen en tussen voertuig en infrastructuur (vehicle-to-vehicle / vehicle-to-infrastructure). Dit niveau omvat authenticatie en toegangscontrole bij draadloze berichten om te bevestigen dat het voertuig communiceert met vertrouwde en geautoriseerde systemen, terwijl de communicatie met andere externe systemen geblokkeerd wordt. Als communicatiekanalen gecreëerd worden met externe systemen moeten die in theorie versleuteld zijn om afluisteren en het invoeren van kwaadwillige berichten te voorkomen.

Beveiliging van niveau 2 (automotive gateway)

controleert al de systemen in de connecteerde wagen. Bestaat uit een 'automotive gateway' die berichten uitwisselt tussen het netwerk in het voertuig en externe apparatuur op niveau 1. Op dit niveau zorgt een filter ervoor dat alleen geautoriseerde berichten tussen de externe systemen en het 'in-vehicle' netwerk uitgewisseld worden. Soms is er sleutelbeheer aanwezig voor de sleutels die de ECU's voor de encryptie en de authenticatie gebruiken. En anomaliedetectie om anomalieën in de beveiliging op te sporen in de berichten die binnen in het voertuig worden uitgewisseld.

Beveiliging van niveau 3 (interne netwerken – 'in-vehicle')

is het netwerk binnen in het voertuig dat berichten uitwisselt tussen ECU's. Het kan in netwerken onderverdeeld zijn volgens de toepassingen en functies van de ECU, zoals telematica voor de navigatie, bediening van de remmen en een body voor de deurvergrendeling. Maakt meestal gebruik van het in-vehicle CAN-protocol voor de communicatie.

Hier treffen we tegenmaatregelen aan, zoals detectie van geknoei, door de berichten die tussen ECU's worden uitgewisseld te wijzigen, en encryptie om afluisteren te voorkomen.

Beveiliging van niveau 4 (hardware, ECU, enz.)

controleert elke individuele component van het voertuig, zoals de motor, de remmen en de deurvergrendeling. Bestaat uit ECU's en andere componenten die een reeks van functies vervullen. Dit niveau omvat het gebruik van veilig ontwerpen en veilige programmeermethoden om menselijke fouten te vermijden en kwetsbare plekken in programma's die op de ECU draaien, alsook een beveiligde systeemstartcontrole om na te gaan of tijdens het opstarten niet met de firmware en het besturingssysteem geknoeid werd.

Boven op de bestaande tegenmaatregelen kunnen nog verscheidene bijkomende technologische oplossingen toegepast worden:

- **Netwerksegmentatie** – Een eenvoudig beveiligingsmechanisme, om congestie op de netwerken van de auto te beperken, fouten tegen te gaan en de algemene veiligheid te verbeteren is het scheiden van de netwerken.

- **Intrusiedetectiesystemen** - geïmplementeerd op veiligheidskritieke systemen die realtime verwerking vereisen.

- **Encryptie van de informatie-uitwisseling** – garandeert dat bij de uitgewisselde informatie de recentste versleutelalgoritmen gebruikt worden, zodat de informatie niet door aanvallers ontcijferd kan worden.

- **Tijdgebaseerde rolling codes** – vooral bruikbaar voor systemen zoals de 'rolling code'. Het kan rolljamaanvallen voorkomen door een tijdgebaseerd systeem van tweewegscommunicatie in te voeren, waarbij de sleutelhanger en de auto gesynchroniseerd blijven door tijdsberichten uit te wisselen. Aangezien de aanvallers het opgevangen signaal niet meteen zullen gebruiken maar wachten op het geschikte moment, zal het tijdbericht in het signaal onveranderd blijven. De auto zal een verschillende tijd hebben, niet meer gesynchroniseerd zijn en de toegang weigeren.

- **Dichten van onnodig geopende poorten en interfaces** – Opdat communicatie kan doorkomen moeten deze poorten geopend zijn, hetgeen normaal is. Dit wordt echter gevaarlijk wanneer poorten onnodig open blijven als gevolg van vergetelheid of lui programmeren. Er is ook een mogelijkheid dat diensten die de poort gebruiken verkeerd geconfigureerd zijn, niet-gepatcht of kwetsbaar voor exploitatie.

8 Aanbevelingen

Volgens de specialisten in cyberveiligheid uit de autosector zijn we voorbij het punt waarop almaar meer hackers in de richting van auto's kijken en de kwaadwillige aanvallen exponentieel gaan toenemen. Dat vraag is niet langer *of* maar *wanneer* bedreigingen van de cyberveiligheid een impact zullen beginnen krijgen in ons dagelijkse leven. De vraag die we ons moeten stellen met betrekking tot de cyberveiligheid in de autosector is niet *of we te laat zijn* maar eerder *of we snel genoeg zijn* om gelijke tred te houden met de indrukwekkende snelheid waartegen de technologie zich ontwikkelt. Met de toenemende aantallen geconnecteerde voertuigen verwachten we ook meer kwetsbare plekken. We zien 5 belangrijke terreinen waarop de overheid het beste haar inspanningen kan richten.

CYBERSECURITY BY DESIGN

De belangrijkste tegenmaatregel bestaat erin problemen te voorkomen: beveiliging vanaf het ontwerp: 'security by design'. Het voertuig moet voor zijn hele levenscyclus beveiligd zijn, tijdens de ontwikkeling, de productie en in de fase van de postproductie. Dat moet de gouden standaard worden, niet alleen voor voertuigen, maar voor alle producten en reglementen die met ICT-technologie te maken hebben. De hele toeleveringsketen in de autosector draagt bij tot de veiligheid van het voertuig. Dus moeten in al die stadia strenge beveiligingspraktijken gelden. Daarom moeten alle betrokken entiteiten aangemoedigd en aangezet worden om voortdurend de nieuwe 'best practices te integreren.

Meerlaagse cyberveiligheidsoplossingen moeten de standaard zijn. Onafhankelijke audits kunnen ook een rol spelen, om te garanderen dat de oplossingen die door de partijen worden toegepast ook up-to-date zijn en in overeenstemming met de recentste regelgeving. Bij de homologatie van voertuigen moet uitgebreid naar de beveiliging gekeken worden, met een methodiek die losstaat van wat de producenten zelf doen.

Het is van belang dat ondernemingen en instellingen het probleem van de cyberveiligheid niet langer kunnen ondermijnen. Volgens een recent onderzoek van EY bij 1.300 professionals in de sector van de cyberveiligheid overweegt 65% van de ondernemingen pas maatregelen op het vlak van cyberveiligheid nadat ze af te rekenen hadden met een aanval. Welnu, reageren op dreigingen is geen optie meer. We moeten erop anticiperen.

NORMEN & REGLEMENTEN

Een grote stap binnen de autosector was de lancering van twee nieuwe reglementen op het vlak van cyberveiligheid voor voertuigen, WP.29 CSMS en SUMS, afkomstig van de Verenigde Naties, en ISO/SAE 21434. De relevante instellingen voor de OEM's, leveranciers van componenten, softwareontwikkelaars en aanbieders van mobiliteitsoplossingen moeten niet langer voorstellen maar eisen dat de nieuwe normen en regels worden toegepast.

Overheden moeten zich achter UNECE, ENISA, de Europese Commissie en de andere relevante instellingen scharen bij de ontwikkeling van nieuwe regelgeving en normen voor de sector. Omdat cyberveiligheid een relatief nieuw domein is schieten de traditionele veiligheidsregels die voorheen in de autosector werden toegepast voortaan tekort. Meer standaardisering is wenselijk maar we moeten overcomplicatie van het proces vermijden, gezien het complexe karakter van de toeleveringsketen naar de autosector. Elke laag daarin kent haar eigen unieke uitdagingen en vereist specifieke methoden die terug te vinden zullen moeten zijn in de nieuwe standaarden. Bovendien moeten we vermijden om binnen het kader van die normgeving het ecosysteem van de cyberveiligheid te centraal te plaatsen opdat geen 'single points of failure' kunnen ontstaan.

CYBERBEWUSTE SAMENLEVING

De grote meerderheid (bijna 80%) van alle aanvallen van het voorbije decennium gebeurden vanaf een afstand en waren dus moeilijker te detecteren en potentieel bedreigend voor meerdere voertuigen tegelijk. Aanvallen van een afstand kunnen aanzienlijk meer en zwaardere schade aanrichten en vergen bijzondere aandacht van de autoriteiten maar ook van de burgers, omdat ze ongemerkt kunnen plaatsvinden.

Om het ecosysteem van de autosector te beveiligen moeten we opleidingen in cyberveiligheid aanmoedigen en elke mogelijke inspanning leveren om de burgers te sensibiliseren rond het belang van het beveiligen van alle geconnecteerde toestellen. Nalatigheid op dat vlak vormt momenteel de grootste bedreiging. Mobiele apps waren tussen 2010 en 2020 de meest gebruikte aanvalsvector, goed voor bijna 10% van alle incidenten. Almaar meer auto's zijn rechtstreeks geconnecteerd met de telefoon via de specifieke mobiele apps (bv. BMW's ConnectedDrive app), hetgeen voor een ernstig risico zorgt wanneer die mobiele telefoons bedreigd worden. Het is van het grootste belang dat alle apparatuur die met het voertuig connecteert up-to-date is en te allen tijde goed beveiligd. Dat kan niet op hoog niveau bereikt worden. Vandaar dat sensibiliseren van het individu hier van cruciaal belang is.

DE MARKT VOORBEREIDEN

Volgens Forbes zijn zo goed als alle autoconstructeurs al het slachtoffer geworden van een cyberaanval – wat aantoont dat cyberdreigingen tot het landschap zijn gaan behoren, niet alleen op het niveau van het individu, maar ook op het niveau van de producenten. Gezien de hoge mate waarin de toeleveringsketen in de autosector een beroep doet op interconnectie, houdt elke verstoring van de veiligheid in dat die toeleveringsketen een significant risico gaat vormen.

Bovendien staan niet alleen OEM's bloot aan cyberdreigingen, maar ook regeringen. Zo werd het Texas Department of Transportation in mei 2020 met ransomware aangevallen. Het probleem blijft echter niet beperkt tot de V.S. alleen. Overheidsorganisaties wereldwijd waren al het doelwit, zoals The National Highways Authority in India, de Kenyase NTSA-portaalsite en in Duitsland een transportvloot van het leger. Het wordt hoog tijd om actie te ondernemen om het ecosysteem te beveiligen, aangezien dat soort incidenten grootschalige gevolgen heeft voor de toekomstige ontwikkeling van de cybercriminaliteit. Almaar meer aandacht gaat naar de incidenten en dat zal wellicht leiden tot nieuwe en ernstigere aanvallen, omdat de mediabelangstelling en het bijbehorende '*prestige*' motiverend werken voor malafide aanvallers.

In de veronderstelling dat OEM's voort softwaregebaseerde upgradeopties zullen blijven gebruiken en ontwikkelen ontstaat hier een enorme markt, legaal en op het 'darkweb'. Dat zal resulteren in een verdere verruiming van het ecosysteem dat al zeer complex is.

Als we nadenken over cyberveiligheid van geconnecteerde voertuigen moeten we het hele ecosysteem bekijken – OEM's en hun hele toeleveringsketen, wagenparkbeheer, diensten voor autodelen, autoverhuurbedrijven, dealers en naverkoopdiensten, verzekeringen en de snelle ontwikkeling van de technologie – in het bijzonder toepassingen binnen *smart cities* die door hun oplossing voor verkeersmanagement enz. een potentiële aanvalsvector creëren die zeer ernstige gevolgen kan hebben.

Vanuit wetgevend oogpunt moeten alle aansprakelijkheids- en garantieaspecten bij aanvallen in de toekomstige wetgeving worden opgenomen, om te voorkomen dat grijze zones ontstaan en de aansprakelijkheid bij schadegevallen versnipperd raakt.

KWETSBAARHEID ≠ OPERATIONEEL RISICO

Hoewel uit onderzoek blijkt dat veel kwetsbare plekken gebruikt zouden kunnen worden, zijn enorme inspanningen vereist om de correcte signalen naar de relevant ECU's te kunnen sturen en een ernstige bedreiging voor de veiligheid te vormen, maar het blijft mogelijk. Er blijven risico's die we niet naast ons neer kunnen leggen, vanwege het zeer grote aantal aanvalsoppervlakken en -vectoren, de lange levensduur van een voertuig en het ontbrekende kader om gedurende de hele levensduur ervan zijn bescherming te garanderen, alsook de algemene blootstellig aan nalatigheid wat veiligheid betreft, zeker bij individuen en met betrekking tot apparatuur die een opening kan bieden naar de systemen in voertuigen.

In het verleden bestond er niet zoveel belangstelling voor het aanvallen van entiteiten uit de autosector. Door de grotere media-aandacht en financiële stimuli kunnen we evenwel verwachten dat vernuftigere methoden zullen opduiken. De kwetsbare plekken die ethische hackers voortdurend blootleggen in het kader van 'bug-bounty'-programma's, geven een idee van de omvang van het probleem. Ethische hackers (white hat) mogen dan wel geen kwade bedoelingen hebben; de kwetsbare plekken die ze blootleggen blijven storend omdat ze potentiële aanvalsvectoren aan het licht brengen. We merken op dat binnen de ethische categorie ook een grijze zone bestaat. 'Grey-hat' hackers hacken niet om kwaad te berokkenen maar om toegang te krijgen tot

dienstverlening zonder de betaalmuur te passeren. Dat heeft een directe impact op de inkomsten van OEM's en dienstverleners.

9 Woordenlijst

TPM	Trusted Platform Module (also known as ISO/IEC 11889): international standard for a secure cryptoprocessor, a dedicated microcontroller (chip) designed to secure hardware through integrated cryptographic keys.
TCP	Transmission Control Protocol: provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network.
UDP	User Datagram Protocol: a simple message-oriented transport layer protocol, which is suitable for purposes where error checking and correction are either not necessary or are performed in the application. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for packets delayed due to retransmission, which may not be an option in a real-time system.
ECU	Electronic Control Unit: any embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle.
CID	Central Information Display
Telematics	A method of monitoring a vehicle. By combining a GPS system with on-board diagnostics it's possible to record – and map – exactly where a car is and how fast it's traveling, and cross reference that with how a car is behaving internally.
Head unit	Automotive infotainment component providing a unified hardware interface for the system, including screens, buttons and system controls for numerous integrated information and entertainment functions.
Cellular connection	Connection established through a mobile network-communication network where the last link is wireless.
CAN bus	Controller Area Network- standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer (message-based protocol).
High speed CAN network	Implemented with two wires and allow communication at transfer rates up to 1 mbit/s.
Low speed CAN network	Implemented with two wires, can communicate with devices at rates up to 125 kbit/s, and offer transceivers with fault-tolerant capabilities.
Kernel	A computer program at the core of a computer's operating system with complete control over everything in the system.
802.1x	IEEE Standard for port-based Network Access Control (authentification)
OBD	On-Board Diagnostics
TCU	Transmission Control Unit
PII	Personally Identifiable Information
OTA	Over the Air Updates
RSU	Road Side Unit
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport -> high speed multimedia network
FlexRay	Automotive network communications protocol: designed to be faster and more reliable than CAN and TTP, but it is also more expensive
DSRC	Dedicated Short Range Communications
C-V2X	Cellular vehicle-to-everything
NFC	Near-field communication
IVI	In-Vehicle Infotainment
GNSS	Global Navigation Satellite System
TARA	Threat Assessment and Remediation Analysis
OEM	Original equipment manufacturer
TSP	Telematics Service Providers

VSOC	Vehicle Security Operation Center



Institut Vias

Chaussée de Haecht 1405
1130 Bruxelles

+32 2 244 15 11

info@vias.be

www.vias.be