De risico's van de 'connecte

Mobiliteit is onlosmakelijk verbonden met de huidige maatschappij. Mensen reizen sneller, verder en vaker. De auto is niet alleen een vervoersmiddel, maar dient ook in allerhande comfort te voorzien. Denk aan navigatie, handsfree bellen en parkeerondersteuning. En ook een verbinding met internet wordt steeds meer regel dan uitzondering. Wat betekenen deze ontwikkelingen voor de veiligheid van de bestuurder?

De techniek van de hedendaagse voertuigen wordt steeds geavanceerder en het eind is nog niet in zicht. Was recent handsfree bellen al een luxe, ondertussen wordt een internetverbinding steeds meer ervaren als noodzaak. De 'moderne mens' wil overal bereikbaar zijn en allerlei media kunnen benaderen. Ook voor de autonoom rijdende auto's is internet en GPS een must, want zonder deze voelsprieten is het sturende autobrein stekeblind. Per 2018 dienen alle nieuwe voertuigen voorzien te zijn van E-call. Dit systeem heeft als doel om snelle hulpverlening op gang te brengen bij een ongeval. Hulpdiensten worden automatisch gealarmeerd, er wordt contact gezocht met het slachtoffer en deuren kunnen op afstand worden ont- of vergrendeld. Een technische ontwikkeling die bijdraagt aan onze veiligheid. Externe netwerken en voertuigen zijn op die manier verbonden: de 'connected car'.

De verbinding met de auto wordt in de meeste gevallen door WiFi of bluetooth gemaakt. Gemak dient de mens; de auto start en gaat ook nog open zonder sleutel - de keyless entry - parkeert zichzelf en seint onderhoudsgegevens naar de fabrikant of dealer. Bovendien kennen sommige merken apps die je op de hoogte houden van olie- en benzinepeil en de plaats waar de auto is achtergelaten. Als wetenswaardigheden in onze informatiegestuurde maatschappij erg vermakelijk, maar wat is de keerzijde van dit amusement?

Risico's De autoindustrie is en blijft volop in beweging. Innovatie staat hoog in het vaandel. De nieuwste modellen auto's veranderen qua uiterlijk, comfort en mogelijkheden. Het creëren van een veilige auto staat hoog op het prioriteitenlijstje en wordt geleid door allerhande richtlijnen en wettelijke eisen op dat gebied. Er bestaat een fundamentele kloof tussen veiligheid (safety) en beveiliging (security). De investeringen die de auto-industrie doet op het vlak van veiligheid staan in schril contrast met de investeringen in beveiliging van vertrouwelijkheid, integriteit en beschikbaarheid van de informatiestromen in de auto. Men voegt allerhande comfort toe, maar investeert onvoldoende in de beveiliging van dat comfort en evenmin in de beveiliging van de internetverbinding van de auto.

Recente voorbeelden laten zien dat de beveiliging in de 'connected car' niet op orde is. Zo werd in 2015 de Jeep Cherokee van Chrysler op afstand gehackt waarbij de auto gelokaliseerd kon worden en de snelheid uitgelezen, maar ook werden remmen geactiveerd of uitgeschakeld en kon bij lagere snelheid de motor worden uitgeschakeld. In 2016 werd ook aangetoond hoe de besturing kon worden overgenomen door een laptop op de auto aan te sluiten. Chrysler moest 1,4 miljoen auto's terugroepen. Vooralsnog is er vooral sprake van 'ethische' hacks. Zo ook bij Tesla wiens model S in 2014 al eens gehackt werd door Chinese studenten en ook in 2016 weer slachtoffer werd van een hack via het WiFi-netwerk. De hackers gijzelden de CANbus en waren zo in staat om op twintig kilometer afstand allerlei functionaliteiten van de auto over te nemen, waaronder de remmen. Voorwaarde om te kunnen hacken was wel dat de webbrowser van de auto in gebruik was.

Besturingssysteem De huidige software van 'connected' auto's is niet (voldoende) aangepast om misbruik van

Foto: Politie

Set waarmee een auto met keyless entry kan worden geopend.

d car’

buitenaf te voorkomen. Door de matige architectuur van de software kunnen kwaadwillenden toegang krijgen tot (gedeeltes van) het besturingssysteem van de auto. Vooralsnog hebben we te maken met een relatief beperkt aandeel ‘connected’ auto’s op het totale wagenpark, maar wat gebeurt er als nagenoeg iedere auto ‘connected’ is? Met de verplichte invoering van de E-call en de mogelijkheden tot connectiviteit van oudere auto’s zijn de gevaren van slechte beveiliging en de daarmee gepaard gaande gevolgen wellicht dichter bij ons bed dan verwacht.

Niet alleen fysieke overname van het voertuig vormt een risico voor de consument en de maatschappij. Iedereen heeft een beeld bij een terroristische aanslag die op afstand wordt uitgevoerd door overname van de besturing van een auto. Alleen wordt door de huidige connectiviteit niet alleen je auto gestolen of overgenomen, maar ook je identiteit. De gevolgen voor de consument zijn daarmee groter dan in eerste instantie verwacht.

Hoe kan het dat we deze problemen met de ‘connected car’ signaleren, maar dat er relatief weinig aandacht voor is? De meest voor de hand liggende is het verdienmodel. Voor het kostenbatenplaatje is het onvoldoende interessant om fors te investeren in beveiliging van connectiviteit. Daar komt bij dat de wettelijke eisen ten aanzien van ‘security’ - zoals aansprakelijkheidsstelling bij kwetsbare software - ernstig achterblijven in vergelijking met ‘safety’. De belangen van de autofabrikanten, maar ook die van wereldwijd bekende softwareontwikkelaars in de miljardenindustrie van de autobranche, zijn aanzienlijk. Combineer dit met onvoldoende besef van het grote publiek over de gevolgen van grootschalige voertuigmanipulatie en een potentieel veelomvattend veiligheidsprobleem is geboren.

Verbetermogelijkheden Welke stappen dienen er gezet te worden om de problemen aan te pakken? Het eerste logische antwoord is een verbetering van de techniek. Veel risico’s op het gebied van cybersecurity zijn het resultaat van zwakheden in software en hardware die kunnen worden uitgebuit om schade te veroorzaken. Het vinden van deze zwakke plekken en het installeren van patches zijn een eerste vereiste om de security te verhogen. We zijn allemaal bekend met updates voor de software van onze telefoons en computers. Vaak bevatten deze updates beveiligingspatches die recentelijk geconstateerde kwetsbaarheden oplossen.

Een tweede oplossingsrichting ligt op het terrein van internationale normering en regelgeving in de autoindustrie. Er is behoefte aan regelgeving om verschillende uiteenlopende cybersecurityrisico’s in deze sector te behandelen, variërend van cybercriminaliteit tot gegevensbescherming en privacy tot het verzamelen van informatie. Aangezien cyberspace en het autoverkeer de ▸

De wettelijke eisen ten aanzien van ‘security’ - zoals aansprakelijkheidsstelling bij kwetsbare software - blijven ernstig achter in vergelijking met ‘safety’.

De autonoom rijdende auto zal ongevallen ten gevolge van dronken automobilisten uiteindelijk uitbannen. Echter, nieuwe faalmechanismen worden geïntroduceerd.

landsgrenzen overschrijden, kunnen landen op nationaal niveau niet zoveel doen. Daarom is regulering op internationaal niveau vereist. In geen geval een eenvoudige uitdaging, gezien de grote verscheidenheid aan culturele, politieke, economische en juridische standpunten over de rol en de aard van cyberspace in de automotive sector.
Op internationaal gebied is er sprake van goede normering van safety. Zo zijn er Safety Integrity Levels, afgekort SILs. De SIL is onderdeel van de IEC 62061 norm voor de machinebouw en van de ISO 26262 norm voor de autoindustrie. De SIL is een normatieve methode voor de beoordeling van elektrische, elektronische en programmeerbare elektronische systemen met betrekking tot de betrouwbaarheid en veiligheid (safety).

Faalveilig Onderdelen van de auto moeten volgens deze normen faalveilig uitgevoerd worden. Dat betekent dat bij een falen geen onveilige situatie ontstaat. Daarom is het veelal nodig om apparatuur redundant en dus meervoudig uit te voeren. De normering van security is minder ver dan van safety. Voor security borging van de elektrische, elektronische en programmeerbare elektronische systemen in een auto zou de ISO 15408 norm aangehouden kunnen worden, hoewel criteria over het gebruik van cryptografische algoritmen in de communicatie tussen CPU, geheugen, input/output, besturingsbussen, databussen en adresbussen in deze norm niet zijn opgenomen. Gebruik van dergelijke algoritmen kunnen misbruik door derden voorkomen. Een verdere integratie tussen bovengenoemde safety en security normeringen in internationaal verband is derhalve gewenst om in het ontwerp van nieuwe auto's (IT-systemen op wielen) inherente veiligheid te borgen. Een dergelijk ontwerpprincipe wordt ook wel 'safety and security by design' genoemd.

Gebruikersgemak De 'connected car' levert ons gebruiksgemak op en tegelijkertijd nieuwe risico's. Om voor- en nadelen tegen elkaar af te wegen, is een toetsingskader gewenst. De autonoom rijdende auto zal ongevallen ten gevolge van dronken automobilisten uiteindelijk uitbannen. Echter, nieuwe faalmechanismen worden geïntroduceerd. Het faalmechanisme door het kwaadwillig menselijk handelen van hackers is bovendien een mechanisme dat een domino-effect kan creëren; het zogenaamde afhankelijk falen. Een hacker die erin slaagt om een kwetsbaarheid van een specifieke auto uit te buiten, zal er waarschijnlijk in slagen om alle auto's van dit type te hacken. Het goed kunnen toepassen van een toetsingskader vereist empirische data.
Hoeveel waardeert een automobilist het extra gebruiksgemak tegenover een uitruil van gebruiksrisico's? Dit soort vragen kunnen pas goed beantwoord worden als er meer casuïstiek beschikbaar komt. De belangrijkste casuïstiek op dit moment zijn de cases van Chrysler uit 2015 en 2016. Deze casuïstiek dient inzicht te verschaffen in de verdeling van verantwoordelijkheid tussen gebruiker, de fabrikant en de overheid. De gebruiker gaat ervan uit dat zijn 'connected car' volledig veilig (safe and secure) is. De fabrikant heeft als doel een zo veilig mogelijke auto op de markt te brengen, maar realiseert zich dat oneindige veiligheid onmogelijk is. De overheid onderzoekt met keuringsdiensten de veiligheid van het wegverkeer en geeft pas vergunningen af zodra de techniek veilig genoeg is. Bovendien verwacht zij dat de automobilist zich in de auto niet laat afleiden door de vele nieuwe gebruiksmogelijkheden. De juridische invulling van dit verantwoordelijkheidsvraagstuk is onderwerp van discussie en zal de komende jaren verder vorm moeten krijgen.

■ Christian Doerr & Pieter van Gelder (TU Delft)
Dirk in 't Hout & Susan Wubbels (Politie)
Redactie@beveiliging.nl