Hoe kwetsbaar is voertuigelektronica?

Auto-inbraak 2.0

Draadloos software-updates uitvoeren, voertuigen op afstand uitlezen en coöperatief rijden zijn technieken in opkomst. Ze bieden straks meer gemak voor werkplaats en eigenaar. Maar ze brengen ook een risico met zich mee. Wie heeft er allemaal toegang tot de auto en hoe (on)veilig is dat?

Echt of fake? Door overbelasting van de CAN-bus komen berichten niet of te laat aan. Daardoor ontstaan storingen.

De afgelopen maand waren verschillende banken het doelwit van zogenoemde DDoS-aanvallen. Dat staat voor Distributed Denial-of-Service. Daarbij gebruiken kwaadwillenden een netwerk van meerdere computers om een computer, netwerk of dienst onbruikbaar te maken door een systeem te overspoelen met berichten. "Iets soortgelijks is ook in een auto mogelijk", zegt Mark van den Brand, hoogleraar Software Engineering & Technology aan de Technische Universiteit Eindhoven. "Overbelasting van de CAN-bus is mogelijk met een DoS-aanval zodat berichten niet of te laat aankomen. DoS staat voor denial-of-service, een aanval met één computer."

Technisch is het dus mogelijk om de auto-elektronica plat te leggen. Maar hoe bereikt een hacker de kwetsbare systemen? Moderne auto's beschikken over allerlei verbindingsmogelijkheden. De meest belangrijke en waarschijnlijk ook de meest kwetsbare is de OBD-aansluiting. Verder beschikken multimediasystemen over een DVD-speler en USB-aansluitingen. Navigatiesystemen halen gegevens van een SD-kaart en steeds meer auto's zijn via het GSM-netwerk met internet verbonden om muziek te streamen of e-mails te downloaden. Het Bluetooth telefoonsysteem, de startonderbreker, TPMS en keyless entry zijn andere systemen die draadloos toegang hebben tot bepaalde auto-elektronica. Genoeg ingangen dus voor een hacker.

Hacken vormt een gevaar

Al die systemen ontzorgen de werkplaats en bestuurder of eigenaar van een voertuig. Volvo introduceerde vorig jaar een systeem waarmee Volvo-trucks op afstand uitgelezen kunnen

Een moderne auto heeft verschillende ingangen. Alleen al het multimedia- en navigatiesysteem beschikt over een DVD-speler, USB-aansluiting, Bluetooth-verbinding en SD-kaartlezer. Gelukkig zijn deze systemen meestal gescheiden van de CAN-bus.

BMW ConnectedDrive ondersteunt de bestuurder. De meeste systemen staan niet direct met internet in verbinding, maar krijgen alle data via de server van de autofabrikant. Die kan zo virussen tegenhouden.

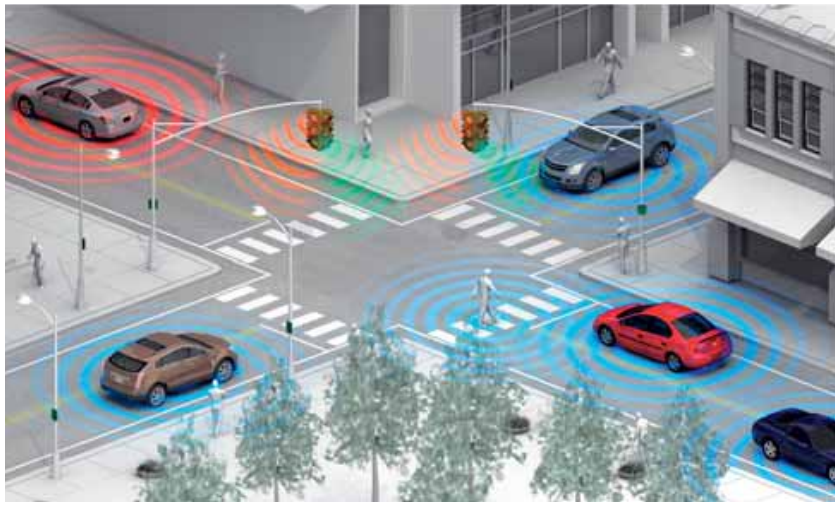
worden. Als de truck op een andere manier wordt ingezet, dan waar het onderhoud op afgestemd is, krijgt de Volvo-dealer een bericht. De dealer neemt dan weer contact op met de klant. Ook andere automerken bieden mogelijkheden om op afstand met auto's te communiceren. Tesla gaat nog een stap verder met de Model S. De firmware van de auto is op afstand te updaten. De auto is daarvoor met internet verbonden. Dat biedt ook mogelijkheden voor kwaadwillenden. Is de angst voor het hacken van een auto terecht? "Zeker", zegt Van den Brand. Toch zijn er nog geen gevallen bekend van gehackte auto's. "De vraag is of gehackte auto's wel het nieuws halen of dat autofabrikanten aanvallen goed geheim weten te houden."

Feit is wel dat er nu al diverse soft- en hardware verkrijgbaar is, om bijvoorbeeld kilometerstanden terug te zetten. Het gebruik daarvan heeft voornamelijk financiële gevolgen. Een tweede gevaar is inbreuk op de privacy. Van den Brand: "De informatie die een auto verzamelt kan interessant zijn voor verschillende partijen. Denk aan een blackbox die ritinformatie opslaat. Die informatie is noodzakelijk voor een wagenparkbeheerder, maar wat als die informatie bij een verzekeringsmaatschappij of bij de overheid terechtkomt? Een verzekeringsmaatschappij kan de tarieven aanpassen op basis van het rijgedrag. En als de overheid beschikt over ritgegevens en rijsnelheid, is het constateren van snelheidsovertredingen nog eenvoudiger. Het is dus belangrijk dat de informatie veilig opgeslagen wordt en dat je vooraf nadenkt over wie er toegang heeft tot de informatie. Op dit moment zijn we met een onderzoek voor DeBeijer Automotive bezig, waarbij leaseauto's op afstand uitgelezen worden. Het uitlezen is technisch geen probleem, maar wie mag er over de uitgelezen informatie beschikken?"

De Tesla Model S maakt gebruik van internet voor het bezoeken van websites en het downloaden van firmware-updates.

Gescheiden netwerk

Als software direct invloed heeft op de besturing of het rijgedrag van de auto, kan dat levensbedreigende gevolgen hebben. In 2010 deden twee Amerikaanse universiteiten onderzoek naar het hacken van auto's. De resultaten zijn schokkend, want het bleek kinderlijk eenvoudig om op afstand een auto te beïnvloeden. Helemaal natuurgetrouw was het onderzoek overigens niet. In de gehackte auto stond een laptop die via de OBD-stekker met de CAN-bus verbonden was. Vanuit een volgauto werden met een andere laptop opdrachten naar de laptop in de gehackte auto gestuurd. Tijdens het onderzoek bleek dat het mogelijk is om de motor of remmen uit te schakelen. Uiteraard geldt hiervoor wel dat er een verbinding moet zijn tussen de software en de ECU. Maar ook die verbinding bestaat al. Van den Brand: "Je hoeft niet perse via de OBD-stekker contact te maken met de ECU. Als je een verbinding maakt met een ander component dat op de CAN-bus is aangesloten en je zorgt dat het component de CAN-bus gaat overbelasten met berichten, dan komen andere berichten niet meer aan". Het multimediasysteem zou een voorbeeld kunnen zijn, vanwege de vele ingangen zoals Bluetooth, internettoegang en SD-kaarten. Gelukkig werkt het systeem meestal via een eigen MOST-netwerk.



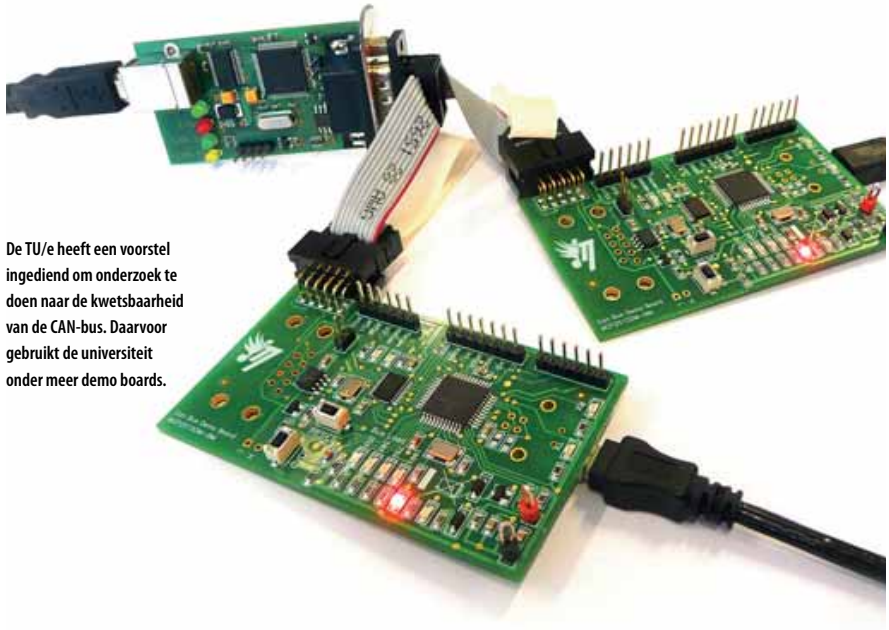
Car-to-X communiceert via de CAN-bus met verschillende componenten. Een goede beveiliging van het systeem is van levensbelang.

Populair systeem is aantrekkelijk

Autosar is een besturingssysteem dat autofabrikanten enkele jaren geleden introduceerden. Het is een universeel systeem, zodat toeleveranciers universele componenten kunnen ontwikkelen die probleemloos aangesloten kunnen worden. Autosar staat voor AUTomotive Open System ARchitecture. "Het feit dat meerdere fabrikanten Autosar gebruiken maakt het systeem kwetsbaar. Kijk naar Windows en Android. Die veelgebruikte systemen zijn een geliefd doelwit voor hackers. Mac OS van Apple is minder wijdverbreid en daarom bestaan daar ook nauwelijks virussen voor", zegt hoogleraar Mark van den Brand. "Als iedereen ziet hoe software werkt, vallen zwakke plekken ook eerder op. Die fout maakte de OV-chipkaart fabrikant Translink. De fabrikant riep dat de kaart niet te hacken is. En wat doe je dan als hacker? Juist, dan ga je op zoek naar mogelijkheden om er wel misbruik van te maken. Als Translink vooraf had aangegeven hoe de chipkaart beveiligd is, was er een open discussie ontstaan en hadden de beveiligingsproblemen meteen aangepakt kunnen worden. Opvallend is trouwens dat er over softwarebeveiliging in auto's ook bijna geen informatie te vinden is. Dat kan twee oorzaken hebben: autofabrikanten doen er niets aan of fabrikanten willen de informatie niet delen. Dat eerste is onwaarschijnlijk en het tweede is onverstandig. Kijk maar naar het voorbeeld van de chipkaart. Op het moment dat bekend is hoe de beveiliging werkt, is er voor hackers geen uitdaging meer."

Toch zijn enkele maatregelen die autofabrikanten nemen tegen het hacken al bekend. Auto's met internettoegang staan meestal niet direct in contact met andere internetservers. Ze hebben alleen verbinding met de servers van de autofabrikant. De autofabrikant filtert dan alle gegevens met een firewall en voorkomt dat virussen de auto bereiken via de internetverbinding.

Autodieven gebruiken voor het stelen van Volkswagens soms het ESP-systeem om toegang tot de ECU te verschaffen. Op die manier kunnen ze sleutelgegevens kopiëren en zonder braakschade een auto openen en starten. Hiervoor geldt dat de dieven wel fysiek bij de auto moeten zijn. Dat geldt niet meer als de auto via Car-to-X communiceert.



De TU/e heeft een voorstel ingediend om onderzoek te doen naar de kwetsbaarheid van de CAN-bus. Daarvoor gebruikt de universiteit onder meer demo boards.

Gevaren beperken

Car-to-X heeft direct toegang tot de CAN-bus en staat draadloos in verbinding met de buitenwereld. Bij coöperatief rijden grijpt de auto in door te remmen en gas te geven. De auto neemt taken van de bestuurder over. De informatie krijgt de auto van voertuigen en computers om zich heen. Maar wat als daar een hacker tussen zit? Die kan onjuiste informatie naar de auto sturen, waardoor de auto bijvoorbeeld gas geeft in plaats van remt. Dat kan grote gevolgen hebben. Volgens Mark van den Brand moeten ontwikkelaars het probleem niet onderschatten: "TNO doet veel onderzoek naar coöperatief rijden. Het is natuurlijk geweldig dat het kan, maar het moet wel veilig gebeuren. Je kunt het nooit 100% beveiligen, maar je kunt wel de gevaren beperken".
De Technische Universiteit Eindhoven wil binnenkort een onderzoek starten naar het hacken van auto's. Van den Brand: "Om mogelijke zwakke punten in een systeem op te sporen, moet je weten hoe hackers te werk gaan. Je zult dus eerst zelf een virus moeten schrijven en vanuit daar kijken wat de mogelijkheden zijn. Die mogelijkheden kun je dan beter gaan beveiligen, maar je kunt niet alles dichtspijkeren. Voor je pc thuis werkt het ook zo. Een anti-virusprogramma kan nooit 100% voorkomen dat je computer gehackt wordt. Anti-virusprogramma's houden je computer constant in de gaten en je moet de software regelmatig updaten om te zorgen dat je veilig kunt blijven werken. We zijn gewend aan updates en misschien moeten we in de toekomst onze auto ook wel regelmatig updaten".
Hoe nu verder? Moeten we ons op dit moment zorgen maken? Nee, de onderzoeken tot nu toe vereisten allemaal fysieke toegang tot een voertuig. In de toekomst gaat dat natuurlijk veranderen omdat veel functies dan ook op afstand benaderbaar zijn. En als een auto op afstand toegankelijk is, ontstaan mogelijkheden om misbruik te maken. Maar technieken zoals Car-to-X en diagnose op afstand zitten nog in de ontwikkelingsfase. Voordat ze daadwerkelijk in nieuwe auto's geïmplementeerd worden, zullen de systemen uitgebreid getest worden. Als later blijkt dat er toch een zwakke plek in het systeem zit, dan voeren fabrikanten gewoon een softwareupdate op afstand uit.

Automotive Technology

Is de angst voor het hacken van een auto terecht? "Zeker", zegt Mark van den Brand, Hoogleraar Software Engineering & Technology aan de Technische Universiteit Eindhoven.

Mark van den Brand, hoogleraar Software Engineering & Technology, geeft Software en System Engineering op de TU. Dat vak maakt onderdeel uit van de master Automotive Technology. Tijdens de colleges van Van den Brand ligt de nadruk op standaardisatie en certificatie.
"De studenten leren niet te programmeren, maar wel hoe software werkt. Daardoor kunnen ze in de toekomst wel met de programmeurs communiceren. De instroom van de studenten aan de master is divers. Er zijn studenten elektrotechniek, werktuigbouw en ICT die de studie volgen."

Autonoom rijden maakt de bestuurder volledig afhankelijk van computersystemen.