TEKST RONALD KAMP

HACKTEST AUTO'S

DIGITAAL LEK OPENT DEUREN

Zijn moderne auto's wel voldoende hack-bestendig? We lieten een Ford en Volkswagen digitaal doorlichten en vonden problemen die je privacy, digitale veiligheid en zelfs je fysieke veiligheid in gevaar kunnen brengen.

Bijna dagelijks worden er kwetsbaarheden gevonden in digitale producten. Auto's zijn tegenwoordig een aaneenschakeling van digitale systemen, zijn ze dan wel veilig genoeg? Voor botsveiligheid en het milieu zijn er allerlei wettelijke eisen, maar op digitaal vlak ontbreken die. Dat actie nodig is, bleek al in 2015 toen beveiligingsonderzoekers de besturing en remmen van een Jeep op afstand deels overnamen. Om de huidige stand van zaken te peilen, lieten we samen met buitenlandse consumentenorganisaties een nieuwe Ford Focus en Volkswagen (VW) Polo hacken. Daarvoor schakelden we het IT-beveiligingsbedrijf ContextIS uit Engeland in.
Eerder vonden we in andere onderzoeken van 'slimme' producten – met een computerchip of internetverbinding – zonder veel moeite flinke veiligheidslekken, bijvoorbeeld bij deurbellen met een camera. Gelukkig blijken niet alle auto's in een vloek en een zucht te kraken. De Ford en VW in onze hacktest

De onderzoekers wisten met een hack de controle te omzeilen en zo aangepaste software te installeren

hebben een stevige 'buitenmuur' die de hobby-hacker wel zal tegenhouden. Maar we vonden na enig spitten wel serieuze veiligheids- en privacygerelateerde aandachtspunten.

Eenmaal binnen...

De IT-beveiligingsonderzoekers die we in de arm namen, ontdekten een grote kwetsbaarheid in het infotainmentsysteem van de VW Polo. Dat is het centrale systeem van onder meer de boordcomputer, navigatie en media.
De software van het systeem kun je updaten, waarbij gecontroleerd wordt of de updates wel origineel van VW zijn. Onze onderzoekers wisten met een hack deze controle te omzeilen en zo aangepaste software te installeren. We hielden de wijzigingen beperkt tot een ander systeemlogo en automatische uitschakeling na vijf minuten.
Het gevaarlijke is dat deze aanpassingen überhaupt mogelijk zijn. Het wijst op een open deur naar veel kwalijkere aanvallen. Het infotainmentsysteem van de Polo zit namelijk samen met andere onderdelen in een computernetwerkje, in de autobranche CAN-bus genoemd. Gelukkig zijn belangrijke aandrijfsystemen, zoals de besturing en remmen, afgeschermd in een eigen CAN-busnetwerk. Een deel van het stabiliteitssysteem (het tractieregelsysteem) blijkt toch te beïnvloeden van buitenaf. Dit zou een kwaadwillende hacker in theorie kunnen uitschakelen met een malafide software-update van het infotainmentsysteem. Daarmee wordt de auto minder veilig. Ook de automatische lichten en ruitenwissers zitten in hetzelfde netwerkje en zijn dus kwetsbaar. Nog een reden waarom aangepaste updates gevaarlijk zijn: ze kunnen malware – bijvoorbeeld gijzelsoftware – binnen brengen of juist gebruikersdata naar buiten, zoals je locatiegeschiedenis en telefooncontacten. Voor een malafide update is wel fysieke toegang tot de auto nodig. Maar een monteur met kwade bedoelingen heeft slechts een paar minuutjes nodig. En ▸

8000

WOORDEN STAAN ER MAAR LIEFST IN DE PRIVACYVOORWAARDEN VAN VOLKSWAGEN

VEILIGHEID VAN SLIMME AUTO'S

De belangrijkste onderdelen van moderne auto's als het om digitale veiligheid gaat, zijn:

1. CAN-BUS. Elke moderne auto heeft een bedraad netwerk, dat is opgedeeld in verschillende subnetwerkjes die we CAN-bus noemen. Aan deze CAN-bussen zijn alle systemen van de auto gekoppeld, van remmen tot richtingaanwijzers.

2. CENTRALE GATEWAY. De CAN-bussen zijn verbonden met elkaar via een firewall of poortwachter: de centrale gateway. Deze bepaalt welke informatie erdoor mag en welke niet. En voorkomt zo bijvoorbeeld dat je via de wifi-verbinding van de auto de besturing kunt beïnvloeden.

3. AANDRIJVING. Moderne auto's hebben diverse CAN-bussen: de Ford Focus heeft er zeven. Die met aandrijvingsonderdelen – zoals besturing en remmen - is een van de belangrijkste. Die onderdelen moeten goed afgeschermd zijn van systemen met een externe aansluiting of draadloze verbinding.

4. INFOTAINMENT. Het centrale informatie- en entertainmentsysteem in een auto is vaak een zwak punt, omdat het altijd externe verbindingen heeft. Voor een hacker biedt dat een aanvalskans en mogelijk ook een toegangspoort naar andere systemen in de auto.

5. MOBIELE APPS. Apps in of gekoppeld aan auto's zijn steeds meer gemeengoed, bijvoorbeeld voor ontgrendelen, voorverwarmen of de accustatus. Ze zijn potentieel kwetsbaar. De Ford Pass en VW Connect apps lijken op veiligheidsgebied in orde.

zelfs iemand zonder sleutel kan je auto binnenkomen, zie het kader 'Autodief gaat met zijn tijd mee'. Ook bij een tweedehandsauto weet je dus niet meer zeker of er kwaadaardige software aanwezig is.

Lekke band?

Bijna iedere nieuwe auto heeft een infotainmentsysteem, en dat is dus een aangrijpingspunt voor hackers. Maar ook iets simpels als de bij nieuwe automodellen verplichte bandenspanningscontrole blijkt soms lek. De communicatie tussen de wielsensoren en de centrale computer in de Ford Focus konden we onderscheppen buiten de auto. Die bleek een unieke identificatiecode te bevatten, waarmee je met uitleesapparatuur langs de weg de auto zou kunnen herkennen. Bovendien denken we dat het mogelijk is om zo de bandenspanningscontrole te beïnvloeden, al hebben we dat niet met 100% zekerheid kunnen bewijzen. Een scenario zou dan zijn dat criminelen je tot stoppen aansporen door de auto te laten denken dat een band lek is. Of je juist door laten rijden terwijl de band wél lek is.

Veel verzamelde data

In moderne auto's zitten talrijke computerchips en enkele kilometers elektrische bedrading. In feite zijn het geavanceerde rijdende mobiele telefoons. De auto heeft al toegang tot je smartphone als je die koppelt en voegt daar eigen camera's en allerlei sensoren aan toe. Bovendien is hij verbonden met het internet of apps. Hij genereert, verwerkt en verzamelt een astronomische hoeveelheid gegevens. Deze digitalisering heeft zeker voordelen, maar net als bij smartphones zijn bedrijven soms wel erg gulzig als het om je persoonlijke gegevens gaat. Wanneer je de Ford App installeert en met je auto verbindt, ga je akkoord met het delen van een heleboel data. Van allerlei auto- en rijgegevens zoals verbruik en bandenspanning tot je locatiegeschiedenis en informatie over versnellen, snelheid en remmen.

Ook bij Volkswagen roepen sommige punten vragen op. Bijvoorbeeld nadat we anoniem onze test-Polo aanschaften en de dealer ons aanspoorde VW's We Connect-app te installeren. Die vroeg om een waslijst aan gegevens van je smartphone, zoals je agenda-afspraken en de inhoud van je bestandsopslag. Dat laatste is volgens Volkswagen bijvoorbeeld nodig voor tijdelijke opslag van bestanden om de app snel genoeg te houden. Bij het doorspitten van de privacyvoorwaarden lazen we dat VW de verzamelde data 'alleen' deelt met derden als dit nodig is vanwege contractuele verplichtingen. Niet echt geruststellend.

Opschonen en ontkoppelen

Door alle digitale techniek bevat je auto een schat aan persoonlijke data. Geef je bolide daarom bij verkoop niet alleen een poetsbeurt, maar schoon ook je gegevens voor zover mogelijk op. Dat dit nodig is, bleek wel toen we een tweedehands infotainmentsysteem van een VW Polo kochten. Dat zat boordevol informatie van de vorige eigenaar. Waaronder zijn telefooncontacten, huisadres en zelfs de inloggegevens van zijn wifi-netwerk.

Let ook op als je een moderne tweedehands auto koopt. Auto's die met een app verbonden zijn, kunnen ongemerkt je locatie nog doorgeven. En bij modellen waarvoor de smartphone als sleutel kan functioneren, blijft de vorige eigenaar die rechten houden als hij niet ontkoppeld wordt. Dat kan de oude of de nieuwe gebruiker doen.

Er is duidelijk actie nodig om de privacy bij moderne auto's te verbeteren. De recente conceptrichtlijn van de Europese privacywaakhond EDPB lijkt een goede stap. Die richtlijn pleit voor vergaande restricties bij het gebruik van zowel voertuig- als gebruikersdata. En voor meer gebruikerscontrole daarop, bijvoorbeeld met een centrale delete-knop.

De autobranche trekt het eigenaarschap van rij- en gebruiksgegevens wel heel makkelijk naar zich toe. Wij vinden dat de automobilist explicieter moet toestemmen, waarbij het bovendien helder en begrijpelijk moet zijn waar hij precies mee instemt. En later moet de toestemming ook in te trekken zijn.

Te veel informatie

Voor de door ons ontdekte kwetsbaarheden moesten onze beveiligingsonderzoekers flink aan de bak. Ford en Volkswagen investeren dus wel op dit punt. Toch zagen we ook slordig programmeerwerk, waaruit blijkt dat de procedures en controles nog wel wat beter kunnen. Zo troffen we bij de Polo veel informatie aan over de technische werking van het info-

2 KM

AAN ELEKTRISCHE BEDRADING IS IN EEN MODERNE AUTO NIET ONGEWOON

Ronald Kamp is redacteur-onderzoeker digitale producten bij de Consumentenbond

'Bij een auto kan de fysieke veiligheid in het geding komen'

'In de autobranche zien we nu een periode met veel veranderingen. Vaak ten goede, maar op privacy- en veiligheidsgebied ontstaan er nieuwe problemen. Zolang er geen goede regelgeving is, moeten we fabrikanten achter de broek aan zitten om hun zaakjes op orde te krijgen. Uiteindelijk kan bij een auto de fysieke veiligheid in het geding komen. Veiligheidslekken moeten we daarom zeer serieus nemen, helemaal omdat de auto steeds meer van onze rijtaken gaat overnemen.'

tainmentsysteem. Deze informatie hielp ons het systeem te kraken en zou eigenlijk niet voor derden inzichtelijk moeten zijn. Nog iets onwenselijks: we vonden enkele jaren oude software-componenten met al bekende kwetsbaarheden. Ook Ford maakt zich schuldig aan het gebruik van verouderde software-componenten. Maar nog kwalijker is dat we inloggegevens voor Fords wifi-netwerk van de Amerikaanse productielocatie aantroffen. Een kwaadwillende kan daarmee mogelijk bij vertrouwelijke

Geef je auto bij verkoop niet alleen een poetsbeurt, maar schoon ook je gegevens op

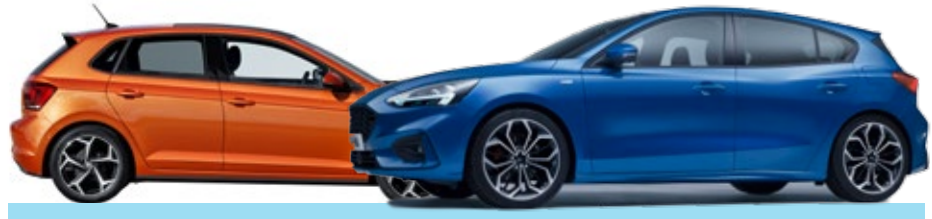
gegevens en wie weet geven die inloggegevens zelfs digitale toegang tot alle auto's die van de band rollen.

Autofabrikanten reageren

We deelden onze bevindingen met Ford en Volkswagen. Volkswagen reageerde coöperatief, maar onderneemt geen actie op alle gevonden kwetsbaarheden. Die leiden volgens de fabrikant niet tot direct gevaar voor de inzittenden en het kost een hacker veel moeite om ze te misbruiken. Op onze geslaagde poging om aangepaste software-updates te installeren, is de reactie van VW dat deze updates niet ongemerkt kritische controlesystemen kunnen beïnvloeden. Toch gaan ze onze bevindingen wel analyseren met de leverancier van het infotainmentsysteem en mogelijk aanpassingen doen.
Ook Ford gaf aan digitale veiligheid zeer serieus te nemen en er continu aan te werken om risico's te verkleinen. Ford ging niet in detail in op alle kwetsbaarheden. Zo wil het bedrijf geen commentaar geven op de door ons gevonden wifi-inloggegevens en wat het mogelijk voor gevolgen kan hebben als kwaadwillenden die vinden. Dit omdat we niet daadwerkelijk met het Amerikaanse fabrieksnetwerk verbonden hebben en daar ook geen toestemming voor hadden. Ford wil hierover niet verder in gesprek met ons. Wat privacy betreft, geeft Ford aan dat de verzamelde data nodig zijn om het geheel goed te laten functioneren, zoals in de voorwaarden staat. VW zegt dat het alleen data verwerkt als de gebruiker heeft toegestemd. Maar wat is dat waard als het alternatief dan is dat je de app of dienst niet kunt gebruiken?

Zorgen voor updates

Sommige van de door ons gevonden kwetsbaarheden lijken misschien triviaal of vergezocht, maar uiteindelijk staat naast de privacy de fysieke veiligheid van inzittenden op het spel. Zeker nu auto's steeds meer zelfrijdend worden, zijn concessies aan de digitale veiligheid uit den boze. Er moet door autofabrikanten dus nog een flinke slag gemaakt worden.
Wij vinden dat er regelgeving moet komen voor met internet verbonden apparaten, waaronder auto's, zodat privacy en veiligheid gewaarborgd zijn. Die is nu gelukkig wel in de maak; wij houden in de gaten of het belang van de consument hiermee voldoende wordt beschermd. Ook moet het updatebeleid bij veel fabrikanten op de schop. Producten moeten gedurende hun gebruiksduur ondersteuning krijgen via veiligheids- en functie-updates. Veel autofabrikanten hebben überhaupt nog geen goed proces ontwikkeld om software-updates snel bij de consument te krijgen. Zeker bij een kritiek probleem is dat geen goede zaak. Ook hierbij houden wij dus de vinger aan de pols.



AUTODIEF GAAT MET ZIJN TIJD MEE

Van hengelen met een ijzerdraadje naar het opvangen van draadloze signalen: de autodief gaat met zijn tijd mee. Digitale methodes om auto's te openen zijn al jaren bekend. Teleurstellend dat een moderne Polo daar vatbaar voor is. Onze onderzoekers konden de ontgrendelsignalen van de afstandsbediening op een apparaatje opslaan, ondanks beveiliging daartegen. Daarmee is de auto later te openen. Zo'n rolljam-aanval is overigens niet heel waarschijnlijk, omdat de crimineel op actie van de eigenaar moet wachten.
Een geavanceerder autoslot heeft zogenoemde keyless entry: de auto gaat open als je ernaast staat met de sleutel op zak. Handig, maar helaas ook voor criminelen. Heel wat auto's zijn gestolen doordat de dieven met een speciale antenne bij de huisdeur gingen staan, en zo het sleutelsignaal tussen huis en auto verlengden tot wel 100 meter. De sleutel in een blikje leggen kan helpen. Onze test-Ford heeft keyless entry, gelukkig met een extra beveiliging. Als de sleutel een tijdje ligt, gaat hij in slaapstand en zendt dan geen signaal meer uit. Dat maakt het lapmiddel met het blikje overbodig.

CHECK ONLINE Kijk voor extra informatie op consumentenbond.nl/autohack

Consumenten bond

Smaakt dit naar meer?

Word lid en krijg direct toegang tot alle onafhankelijke tests en informatie.

Ja, vertel me meer