

Analyserapport

CASUS IOT SECURITY

Finn Alberts, Laurent Dassen, Maud Derhaag
en Brent Vliex
ZUYD HOGESCHOOL | HBO ICT



Inhoud

1 Inleiding.....	3
2 Aanpak	3
3 Resultaten	3
3.1 Architectuur	3
3.2 Beveiligingsrisico's	4
3.3 Privacyrisico's.....	4
4 Conclusie	7
5 Discussie.....	7
6 Verwijzingen.....	7
7 Bijlagen.....	8
7.1 Interview met Volvo-dealer	8

1 Inleiding

Dit analyserapport is onderdeel van het IoT-security project. Binnen dit project zal de beveiliging van een Volvo V60 in combinatie met Volvo On Call worden onderzocht. Binnen dit analyserapport wordt de volledige beveiligingsanalyse beschreven.

2 Aanpak

Allereerst zal de architectuur van de Volvo V60 in combinatie met Volvo On Call worden onderzocht. Hiervoor wordt gebruik gemaakt van desktop research en de reeds uitgevoerde field research.

Nadat deze architectuur in kaart is gebracht kunnen de beveiligingsrisico's worden onderzocht. Hiervoor wordt gekeken naar de architectuur en waar mogelijk kwetsbare plekken zitten.

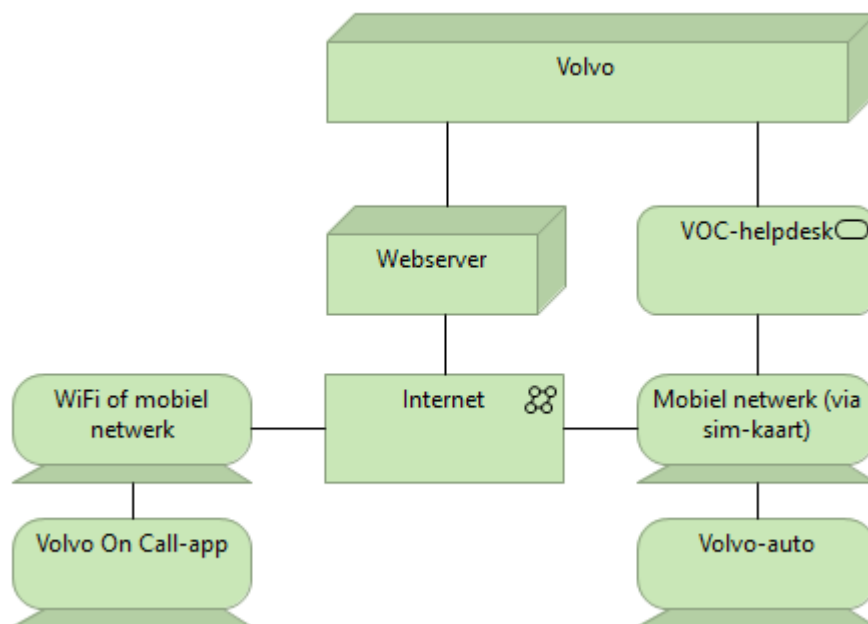
Vervolgens zal nog worden onderzocht welke privacyrisico's ontstaan door Volvo On Call bij het doorverkopen van de Volvo V60. Ook hiervoor zal met name worden gekeken naar de architectuur en gebruik worden gemaakt van desktop research.

Mochten er privacy- of beveiligingsrisico's worden gevonden, dan zal worden nagedacht over een oplossing. Hiervoor wordt optioneel nog gebruikgemaakt van desktopresearch.

3 Resultaten

3.1 Architectuur

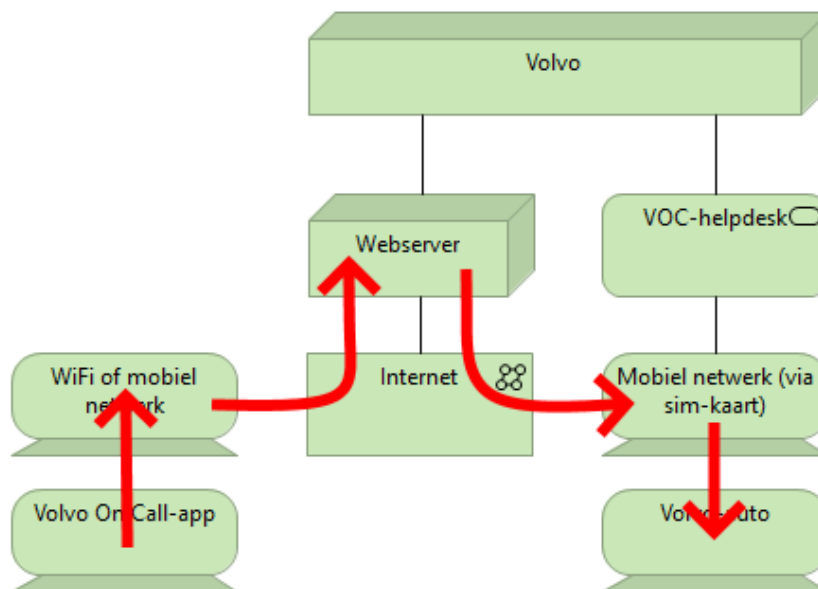
De architectuur die de Volvo V60 gebruikt voor Volvo On Call is te zien in Figuur 1.



Figuur 1 Volvo On Call-architectuur

Zoals in de figuur te zien is maakt de auto uitsluitend via een mobiel netwerk verbinding met internet. Dit blijkt uit de volgende quote *“Met Volvo On Call verbindt u uw Volvo via een simkaart met internet. Zo beschikt u over in-car wifi waar u ook heengaat.”* uit een Volvo-brochure (Volvo, 2018). Dit wordt tevens, met enige twijfel, bevestigd door een Volvo-dealer, zie 7.1 Interview met Volvo-dealer.

Wanneer de gebruiker via de mobiele applicatie bijvoorbeeld de lampen aan wil zetten van zijn/haar Volvo, zal de app via WiFi of het mobiele netwerk verbinding maken met internet. Het verzoekje zal worden doorgestuurd naar een webserver. Vervolgens zal de webserver via internet en het mobiele netwerk een verzoek naar de Volvo sturen. Zie voor een visuele weergave van hoe dit verzoek wordt verstuurd Figuur 2.



Figuur 2 Verzoek vanuit mobiele app bij Volvo On Call

Het bewijs dat de mobiele applicatie geen directe verbinding maakt met de auto, maar dit via een webserver gaat, is dat Volvo een privacyverklaring heeft opgesteld met daarin welke gegevens ze opslaan en wie hier toegang tot heeft (Volvo, 2020). Dit laat zien dat de gegevens niet in eigen beheer (opgeslagen in de auto) zijn.

In de architectuur is ook de Volvo On Call-helpdesk te zien. De helpdesk maakt telefonisch contact met de auto op het moment dat de airbags afgaan of wanneer de gebruiker op een speciale knop hiervoor drukt. Volgens 7.1 Interview met Volvo-dealer wordt dan ook de locatie van de auto gestuurd om zo, indien nodig, hulp te kunnen sturen.

3.2 Beveiligingsrisico's

Tijdens het onderzoek naar de beveiliging van Volvo zijn er geen beveiligingsrisico's kunnen worden geconstateerd. In het testrapport is te zien hoe de projectgroep te werk is gegaan met het onderzoeken naar welk dataverkeer er tussen de Volvo On Call-app en de Volvo auto is. Uit deze test hadden beveiligingsrisico's kunnen komen. Omdat de test geen concrete resultaten heeft gegeven, kunnen er geen beveiligingsrisico's worden geconstateerd.

3.3 Privacyrisico's

Zoals in de architectuur beschreven is in hoofdstuk 3.1 Architectuur, wordt er bij Volvo On Call gebruik gemaakt van een webserver. Deze webserver wordt gebruikt voor alle communicatie met betrekking tot Volvo On Call. Dat wil zeggen dat op deze webserver de verzoeken binnenkomen voor het aan- of uitzetten van de lampen.

Ook worden persoonsgegevens verzameld en opgeslagen op de webserver. Deze gegevens worden opgeslagen om toegang te kunnen verlenen bij het aanmaken en gebruiken van Volvo services, zoals Volvo ID en Volvo On Call.

Gegevens als voornaam, achternaam, telefoonnummer, voorkeurstaal, land, e-mail en wachtwoord worden opgeslagen in de webserver. Een risico dat zich hierbij kan voordoen is dat de webserver wordt gehackt. Wanneer deze gegevens in handen komen van criminelen kan dit voor identiteitsfraude zorgen (Volvo, 2021).

Naast de persoonsgegevens worden er ook andere gebruikersgegevens opgeslagen. Deze gegevens worden automatisch opgeslagen wanneer er een gebeurtenis met de Volvo On Call app wordt uitgevoerd.

Deze informatie bestaat uit het voertuigidentificatienummer (VIN), het tijdstip dat de dienst wordt aangeroepen, het type dienst, of er airbags en/of gordelspanners zijn geactiveerd, de actuele hoeveelheid brandstof, de actuele temperatuur in en om de auto, of portieren/deksels/kleppen en ruiten vergrendeld of ontgrendeld zijn en de zes laatst bekende locaties van de auto (Volvo, 2020).

Ook informatie over telefoontjes met inzittenden, de helpdesk en de aantekeningen die de helpdeskmedewerker maakt worden opgeslagen (Volvo, 2020).

Aan het opslaan van deze gegevens zit ook een risico. Wanneer criminelen toegang krijgen tot de webserver, kunnen ze bijvoorbeeld volgen waar de auto is en dit kan heel gevaarlijk zijn. Ook kan er bijvoorbeeld gezien worden of iemand vergeten is de auto te vergrendelen.

Voor alle genoemde gegevens gelden verwijderingsprocedures. Gegevens die opgeslagen zijn in verband met de gebeurtenissen met de Volvo On Call-app dienen uiterlijk 100 dagen nadat ze opgeslagen zijn verwijderd te worden. De persoonsgegevens die aan de bovengenoemde Volvo Services zijn verbonden, blijven ten minste de hele contractduur opgeslagen. Daarna worden ze nog opgeslagen zolang dat nodig is voor Volvo On Call om te voldoen aan wettelijke en andere verplichtingen (Volvo, 2020).

Een risico wat hieraan vastzit is dat er nog 100 dagen extra zijn om niet legitiem bij de gegevens te komen. Ook worden hierdoor meer gegevens opgeslagen.

In de handleiding over Volvo On Call staat dat Volvo de dienstverlening uitbestedt aan partners. Er staat echter niet bij om welke partners het gaat. Deze partners mogen de persoonsgegevens inzien en verwerken voor zover dat nodig is voor de dienst die zij uitvoeren. Daarbij hebben de partners een contract met Volvo getekend dat zij, zoals bij wet is vastgelegd, vertrouwelijk omgaan met de persoonsgegevens (Volvo, 2021).

Onder het kopje “Marketing” in de privacyverklaring over Volvo On Call staat dat Volvo persoonsgegevens niet zal verhandelen of verkopen aan derden, tenzij hier akkoord voor is gegeven. Ook zal Volvo geen persoonsgegevens delen met derden voor hun marketingdoeleinde zonder toestemming. Als men toestemming heeft gegeven maar dit niet meer wil, word je doorverwezen naar de derde partij (Volvo, sd).

Bij het verwerken van persoonsgegevens komen altijd privacyrisico's om de hoek kijken. Om de consument een zo goed mogelijk gevoel te geven en om er voor te zorgen dat de verwerking zo goed mogelijk verloopt volgens de wet, heeft Volvo een aantal rechten van de AVG toegekend aan de consument. Dit zijn:

- Het recht uw goedkeuring in te trekken: wanneer er toegang is verleend tot persoonsgegevens kan dit op ieder moment weer worden ingetrokken.
- Het recht op toegang van uw persoonsgegevens: er wordt altijd toegang verleend wanneer eigen persoonsgegevens ingezien willen worden.
- Recht op rectificatie: rectificatie van persoonsgegevens kan worden aangevraagd indien deze niet up-to-date zijn of onjuist.
- Recht op beperking: het is mogelijk om het verwerken van persoonsgegevens te beperken indien er bezwaar is tegen deze verwerking.
- Recht op overdraagbaarheid: het is mogelijk om Volvo te verzoeken om persoonsgegevens te laten delen met of over te laten dragen aan andere partijen.
- Recht op wissing: consumenten hebben het recht om Volvo te verzoeken om persoonsgegevens te wissen.
- Recht van bezwaar: consumenten mogen op elk moment bezwaar maken tegen Volvo en het gebruik van persoonsgegevens.
- Recht op het indienen van een klacht: de consument heeft altijd het recht om een klacht in te dienen bij de gegevensbeschermingsautoriteit.

Met deze rechten zouden consumenten meer te zeggen moeten hebben over wat er gebeurt met hun persoonsgegevens. Ook kunnen ze actie ondernemen wanneer ze het ergens niet mee eens zijn (Volvo, 2021).

Kopen of verkopen van een auto met Volvo On Call

Het is duidelijk dat Volvo voor de Volvo On Call-service redelijk wat persoonsgegevens verzamelt en deze ook verwerkt. Wanneer de auto wordt doorverkocht is het ook belangrijk dat persoonsgegevens en andere privacygevoelige gegevens worden verwijderd. Volvo heeft een handleiding geschreven met instructies voor het resetten van de auto, wanneer deze Volvo On Call gebruikte (Volvo, 2020). Deze handleiding bevat instructies voor zowel de koper als de verkoper van de auto. De instructies voor de verkoper zijn als volgt:

1. Neem contact op met een Volvo-dealer om het Volvo On Call-abonnement stop te zetten. De dealer zal de Volvo On Call-geschiedenis ook verwijderen.
2. Reset de auto naar de fabrieksinstellingen. Dit kan via de instellingen van de auto.
3. Verander het Volvo ID niet. Verbreek wel de link tussen de auto en de Volvo On Call-app.

Wanneer de nieuwe eigenaar ook gebruik wil maken van Volvo On Call neemt hij/zij contact op met de Volvo-dealer. De dealer zal het abonnement overzetten naar de nieuwe eigenaar en eventuele overgebleven data van de vorige eigenaar verwijderen. De nieuwe eigenaar krijgt vervolgens een viercijferige pincode van de Volvo-dealer. Deze pincode is nodig voor het identificeren als eigenaar van de auto.

Uit het interview bij 7.1 Interview met Volvo-dealer is gebleken dat de Volvo-dealer uitsluitend het gekoppelde Volvo ID kan zien bij een auto en geen verdere gegevens van een klant. Dit ID wordt bij doorverkoop dan van de auto verwijderd. Wanneer een Volvo-dealer een auto terugkrijgt of doorverkoopt, wordt het Volvo ID van de vorige klant altijd verwijderd, ook als de klant hier zelf niet specifiek om vraagt.

4 Conclusie

Door onderzoek te hebben gedaan naar de architectuur van de Volvo auto en de Volvo On Call-app is een model gemaakt van de infrastructuur in Figuur 1. Dit heeft bewezen dat de Volvo On Call-app geen directe verbinding maakt met de auto, maar dat de app dit doet via het internet. Deze conclusie is ook getrokken vanwege het feit dat de auto verbinding maakt met een mobiel-netwerk via een simkaart.

Doordat er weinig gegevens konden worden opgehaald, kunnen geen harde conclusies over beveiliging worden getrokken. Op basis van de gegevens die konden worden opgehaald, zijn geen beveiligingsrisico's gevonden. Het is dus ook niet bekend of er maatregelen moeten worden genomen.

Volvo On Call slaat de gegevens op een webserver op. Op deze webserver staan dus gegevens zoals de locatie van de auto. De gegevens op de webserver zijn gekoppeld aan een Volvo ID. Dit ID is vervolgens weer gekoppeld aan de auto.

Wanneer de auto wordt doorverkocht, kan contact op worden genomen met de dealer. De dealer verwijderd vervolgens het Volvo ID wat aan de auto gekoppeld is, zodat de link wordt verbroken. De dealer kan zelf geen gegevens van een klant inzien (buiten het ID).

Wanneer de Volvo auto crashsensoren of de airbags afgaan, krijgt Volvo wel een bericht met de locatie van de auto en zal de Volvo On Call-helpdesk direct telefonisch contact maken met de auto om te zorgen voor de veiligheid van de inzittenden.

Over het algemeen kan dus worden gezegd dat de privacy goed wordt beschermd en er dus geen maatregelen hoeven worden genomen.

5 Discussie

De architectuur kan niet honderd procent gevalideerd worden. Wel is de door de projectgroep opgestelde architectuur het meest aannemelijk, op basis van de informatie die bekend is.

Er zijn door de projectgroep geen beveiligingsrisico's geconstateerd. Het is echter mogelijk dat deze er wel zijn, maar in dit project zijn ze niet gevonden.

De gevonden informatie is voornamelijk van de Volvo sites zelf afkomstig. Het is niet zeker of deze informatie ook daadwerkelijk klopt en nog up-to-date is. Wel is een deel van de gevonden informatie op deze sites, gevalideerd door een Volvo-dealer in een kort telefonisch interview. Dit interview is te zien in 7.1 Interview met Volvo-dealer. Daarnaast zijn dit voornamelijk juridische documenten, die vanwege wetgeving accuraat moeten zijn.

6 Verwijzingen

Volvo. (2018, augustus). *Volvo On Call - De sleutel tot uw digitale wereld*. Opgehaald van Volvo: <https://assets.volvocars.com/nl/~media/netherlands/documents/brochures/overig/volvo-on-call-brochure-my19---web.pdf?la=nl-nl#:~:text=Met%20Volvo%20On%20Call%20verbindt,wifi%20waar%20u%20ook%20heengaat.&text=U%20kunt%20uw%20Volvo%20altijd,eigen%20smartpho>

Volvo. (2020, juli 10). *Buying or selling a car with Volvo On Call*. Opgehaald van Volvo:
<https://www.volvocars.com/in/support/manuals/v60/2018w46/volvo-on-call/practical-information-on-volvo-on-call/buying-or-selling-a-car-with-volvo-on-call>

Volvo. (2020, juli 10). *Personal information and Volvo On Call*. Opgehaald van Volvo:
<https://www.volvocars.com/in/support/manuals/v60/2018w46/volvo-on-call/practical-information-on-volvo-on-call/personal-information-and-volvo-on-call>

Volvo. (2021, mei 31). *Privacy Notice – Volvo Cars App*. Opgehaald van Volvo:
<https://www.volvocars.com/in/legal/privacy/privacy-voc>

Volvo. (2021, mei 31). *Privacy Notice – Volvo ID*. Opgehaald van Volvo:
<https://www.volvocars.com/in/legal/privacy/privacy-volvo-id>

Volvo. (sd). *Customer privacy policy*. Opgehaald van Volvo:
<https://www.volvocars.com/in/v/legal/privacy>

Volvo Rutten. (sd). *Volvo Rutten - Dé Volvo Dealer van Limburg en Z/O Brabant*. Opgehaald van Volvo Rutten: <https://www.autobedrijfritten.nl/>

7 Bijlagen

7.1 Interview met Volvo-dealer

Op 24 juni 2021 is een kort telefonisch interview gehouden met een Volvo-dealer van Volvo Rutten te Boxmeer (Volvo Rutten, sd). Dit is (met toestemming) opgenomen en hieronder uitgeschreven.

Interviewer: Eigenlijk de eerste de vraag die wij hadden, wij lazen online dat wanneer zo'n auto met Volvo On Call wordt doorverkocht dat er contact kan worden opgenomen met de dealer om eigenlijk de geschiedenis te verwijderen van het Volvo On Call-systeem van de vorige eigenaar zoals de locatiegeschiedenis die die auto heeft opgeslagen van hem of haar en we vroegen ons af hoe gaat dat eigenlijk in z'n werk. Zijn er een aantal acties of is er letterlijk een delete-knop induwen en alle gegevens zijn verwijderd van die klant?

Dealer: Nou, wij kunnen geen locatie zien. Wij kunnen alleen zien welke ID gekoppeld is en die kunnen we verwijderen.

Interviewer: Dus u kunt eigenlijk alleen aangeven van dit ID wil ik verwijderen bij deze auto?

Dealer: Ja, ja, voor de rest kunnen wij helemaal niks zien aan die auto.

Interviewer: Dus u kunt zelf ook geen gegevens inzien van die auto. Alleen het ID wat gekoppeld is?

Dealer: Nee alleen het ID wat gekoppeld is.

Interviewer: En wordt dat ook regelmatig gevraagd om die gegevens te verwijderen of heeft u het idee dat dat eigenlijk vaak vergeten wordt?

Dealer: Als wij zelf een auto ingeruild krijgen, dan wordt die sowieso verwijderd, die ID. Dus dan is het systeem leeg.

Interviewer: Oké. Dat klinkt in ieder geval als een goede beveiliging als ik dat zo hoor. Worden die gegevens dat u weet vanuit Volvo nog met iemand anders gedeeld dan eigenlijk dan puur voor de doelen van zelf de gegevens uit kunnen lezen als klant. Zeg maar, ik heb een auto en ik wil de locatie

uit kunnen lezen, wordt de locatie nog met iemand anders gedeeld? Of andere gegevens die die auto opslaat?

Dealer: Locatie wordt alleen gedeeld als er een ongeluk gebeurt. Dat is wat ik weet.

Interviewer: Dus eigenlijk heel streng. Van Volvo deelt dat niet met een partner ofzo?

Dealer: Stel dat er een ongeluk gebeurt en de crashsensors zijn geactiveerd dan wordt er een positie verstuurd.

Interviewer: Oké. Wij lazen ook in een brochure van Volvo On Call dat eigenlijk die auto uitsluitend verbinding maakt via een simkaart met het internet, en dus ook niet via WiFi. Kunt u dat bevestigen of ontkrachten? Of heeft u daar geen antwoord op?

Dealer: On Call weet ik niet, nee. Volgens mij werkt dat inderdaad alleen via een sim.

Interviewer: Oké, en de laatste vraag die we eigenlijk nog hadden. Eigenlijk die gegevens, zoals de locatie die de auto constant blijft opslaan, worden neem ik aan ergens online bij Volvo opgeslagen.

Dealer: Goede vraag. Durf ik niet te zeggen. Lijkt me wel. Met de app kun je zien waar de auto staat. Ik weet niet hoe dat opgeslagen wordt.

Interviewer: Nee, oké. Dat waren eigenlijk al de korte vraagjes die wij hadden. Daar kunnen wij in ieder geval een heel stuk mee vooruit, dank u wel.

Dealer: Nee, oké is goed

Interviewer: Dan wens ik u nog een hele fijne dag verder en werk ze nog.

Dealer: Oké dankjewel, zelfde.