Spookfiles A58

Spookfiles A58

FAQ: (Data)veiligheid en privacy

De kracht van de spookfiledienst die in het project Spookfiles A58 is ontwikkeld, is dat de deelnemers een in-car advies *op maat* krijgen. Om zo'n gepersonaliseerde dienst mogelijk te kunnen maken, is echter veel data nodig. Het gaat daarbij onder meer om heel specifieke gegevens over de voertuigen van de deelnemers: hun locatie, snelheid, richting enzovoort. Welke issues op het gebied van (data)veiligheid en privacy spelen hierbij? En hoe gaat Spookfiles A58 ermee om?

Over Spookfiles A58

De provincie Noord-Brabant is opdrachtgever van het project Spookfiles A58, dat onderdeel is van het programma Beter Benutten van het Ministerie van Infrastructuur en Milieu. Bedrijven, overheid en kennisinstellingen werken in dit project samen aan de introductie van coöperatieve systemen en diensten. Op de A58 tussen Tilburg en Eindhoven zijn daarvoor inmiddels 34 wegkantbakens geplaatst die zijn uitgerust met WiFi-p. Hiermee kan draadloos met geschikte apparatuur in passerende auto's worden gecommuniceerd.

De eerste dienst die op dit systeem draait, is de spookfiledienst: op basis van nauwkeurige informatie over stremmingen en filegolven op het proeftraject krijgen deelnemers gepersonaliseerde *in-car* snelheidsadviezen. Dat maakt dat zij beter op nog niet zichtbare situaties voor hen kunnen anticiperen en daardoor prettiger en soepeler door het verkeer kunnen bewegen.

(DATA)VEILIGHEID

Welke issues spelen er op het gebied van (data)veiligheid?

Als er met data wordt gewerkt – en zeker als er data verzonden worden – spelen er drie typen bedreigingen op het gebied van de veiligheid van de data. Allereerst is er de vraag of de ***authenticiteit*** is gewaarborgd. Bijvoorbeeld: kan ik er als afnemer van een in-car service op vertrouwen dat de informatie op het scherm van mijn apparaat echt afkomstig is van mijn serviceprovider?[1] Ten tweede is er de ***integriteit***. Is het advies dat op mijn schermpje verschijnt juist? Is er niet bewust of onbewust iets aan de data veranderd? En ten derde is er de zorg over de ***beschikbaarheid***. Doet de dienst het wel als ik die wil gebruiken? Of doet er zich ergens in

[1] Soortgelijke problemen spelen natuurlijk ook voor de andere partijen die bij de dienst betrokken zijn, zoals de serviceprovider zelf (zijn de data die de serviceprovider terugkrijgt wel van zijn afnemers?), de verkeerscentrale etc. We beperken ons hier tot voorbeelden van de eindgebruiker.

de keten een probleem voor met het inwinnen of delen van gegevens en leidt dat tot ‘uitval’ van de dienst?[2]

Zijn die issues te voorkomen?

Er bestaat niet zoiets als 100% (data)veiligheid. Het doel van veiligheidsmaatregelen is dan ook om risico’s tot een *aanvaardbaar niveau* terug te dringen. Wat aanvaardbaar is zal van toepassing tot toepassing verschillen. Het spreekt voor zich dat een dienst die de rijtaak (deels) overneemt grotere risico’s met zich meebrengt en dus veel strakker beveiligd moet worden dan een dienst die alleen in informatie of adviezen voorziet.

Wat zijn de veiligheidsrisico’s in specifiek het project Spookfiles A58?

Die zijn klein, omdat de spookfiledienst die wordt aangeboden een adviesdienst is. Het ergste wat er kan gebeuren is dat er een verkeerd advies op het scherm van het apparaat in de auto verschijnt (een advies om snelheid te minderen terwijl dat niet nodig is bijvoorbeeld) of dat er even géén advies binnenkomt. In beide gevallen zit de bestuurder ‘ertussen’ en die zal altijd zijn eigen beslissing nemen.

Uiteraard zijn zulke problemen wel onwenselijk, al was het maar omdat elk issue schadelijk is voor het vertrouwen in (en daarmee: het succes van) het coöperatieve systeem en de spookfiledienst.

Welke (data)veiligheidsaanpak is in Spookfiles A58 gekozen?

Spookfiles A58 is een gezamenlijk ontwikkel- en proefproject voor ITS. Daarom is besloten om ervaring op te doen met geavanceerde (data)beveiligingsmaatregelen. Die zijn geschikt voor de spookfiledienst, maar met name bedoeld voor de toekomst en nog te ontwikkelen diensten.

De belangrijkste maatregel is dat alle berichten die wegkantstations en coöperatieve apparatuur in auto’s verzenden, digitaal worden ondertekend. Dit waarborgt de ***integriteit*** en ***authenticiteit*** van de communicatie, met andere woorden of data daadwerkelijk onveranderd zijn doorgestuurd en afkomstig zijn van een betrouwbare bron Het proces van ondertekenen en controleren wordt aangeduid met de term *Public Key Infrastructure*, kortweg PKI – zie voor een toelichting hierop onderstaande vraag.

Om de ***beschikbaarheid*** optimaal te houden, draait het Spookfiles A58-systeem op kwaliteitsservers met een hoge ‘uptime’.

Hoe werkt het gebruikte PKI-systeem?

Elke systeem in Spookfiles A58 dat draadloos berichten verzendt – dat zijn de wegkantbakens en de coöperatieve apparaten in auto’s – krijgt twee typen digitale ‘sleutels’: geheime sleutels voor die bakens en apparaten en een publieke sleutel die via een database voor iedereen toegankelijk is. Op de uitgifte en registratie van de sleutelsets wordt streng toezicht gehouden.

[2] De veiligheidsproblemen rond de opslag van data (kunnen onbevoegden zich geen toegang verschaffen) bespreken we in het deel over Privacy.

Stel nu dat een serviceprovider een snelheidsadvies wil versturen. Vóór verzending ‘ondertekent’ de serviceprovider dit bericht met zijn ***geheime sleutel***: op basis van de inhoud van het bericht ***genereert*** de sleutel een ***digitale handtekening***. Zodra een coöperatief apparaat in een auto dit snelheidsadvies oppikt, zal het de ***publieke sleutel*** van het zendende wegkantbaken opzoeken. Met deze publieke sleutel kan de ***handtekening*** onder het bericht worden ***gecontroleerd***: is die handtekening wel met de juiste geheime sleutel gegenereerd (= is de afzender wel wie ze beweert te zijn) en matcht die met de inhoud van het bericht? Komt er een ‘OK’ terug, dan weet het coöperatieve voertuigapparaat dat zowel de authenticiteit als de integriteit in orde zijn. Komt er een ‘false’ terug, dan is óf de verzender niet wie ze beweert te zijn of is het bericht gewijzigd.

Maakt het PKI-systeem in Spookfiles A58 gebruik van encryptie om de berichten onleesbaar te maken?

Nee. De reden is heel eenvoudig: de kern van een coöperatief systeem is nu juist het samenwerken en het vrij delen van gegevens tussen de verschillende componenten binnen het systeem (dus: tussen de voertuigapparaten onderling, en tussen die apparaten in de auto’s en de wegkantbakens). Versleuteling van data staat haaks op dat principe en ze dient voor collectieve toepassingen als snelheidsadviezen ook geen enkel doel.

Dat betekent dat bijvoorbeeld snelheidsadviezen vanuit de serviceprovider of locatie- en snelheidsgegevens vanuit voertuigen in principe voor iedereen te ‘lezen’ zijn. Voor de *veiligheid* is dat geen probleem – zolang er maar geen onjuiste of onterechte berichtjes worden verstuurd – maar het roept natuurlijk wel enkele *privacy*-issues op. Zie hiervoor de sectie “Privacy” verderop.

Hoe staat het met (data)veiligheid als er meer diensten beschikbaar komen op het coöperatieve systeem?

Bij elke nieuwe dienst zal gekeken moeten worden of de bestaande maatregelen nog toereikend zijn voor eventuele (nieuwe) risico’s. Waar nodig zal dan in extra beveiliging moeten worden voorzien.

PRIVACY

Welke issues spelen er op het gebied van privacy?

Er worden data verzameld en opgeslagen over onder meer afzonderlijke voertuigen, zoals locatie en tijdstip. Bepaalde informatie wordt ook gedeeld met derden. Dat zijn de eerste risico’s: kunnen er geen onbevoegden bij de data en wordt erop toegezien dat er geen privacygevoelige informatie wordt gedeeld?

Dan is er het punt dat het berichtenverkeer niet wordt versleuteld, omwille van het open en collectieve karakter van het coöperatieve systeem. Theoretisch gesproken zou daardoor ook iemand anders de berichten dus kunnen ontvangen en meelezen.

Hoe worden de privacyrisico's van het opslaan en delen van (voertuig)data tot een minimum beperkt?

Alle brondata die voor het project Spookfiles A58 worden verzameld, worden opgeslagen op servers in zogenaamde serverparken, die zowel fysiek als digitaal stringent beveiligd worden.

De verzamelde data zijn vanuit verkeerskundig oogpunt interessant voor 'derde partijen', omdat ze een nauwkeurig beeld verschaffen over bijvoorbeeld de snelheid en stabiliteit van de verkeersstromen. Om te voorkomen dat derden kunnen inzoomen op afzonderlijke voertuigen, zullen de gegevens alleen *geaggregeerd* aangeboden worden. Daarnaast kunnen de kop en staart van elke individuele rit verwijderd worden. De begin- en eindpunten zijn namelijk nauwelijks te aggregeren en om te voorkomen dat er dan toch informatie over afzonderlijke ritten wordt gedeeld, kunnen de laatste paar honderd meter er worden afgeknipt.

Alle berichten zijn af te vangen en mee te lezen. Tot welke specifieke privacyrisico's leidt dat en hoe worden die afgevangen?

Aan de data die serviceproviders verspreiden via de wegkantsystemen, kleven geen privacyproblemen: het gaat om snelheidsadviezen en waarschuwingen vergelijkbaar met meldingen die ook op matrixborden kunnen worden weergegeven.

Met het dataspoor dat de on-board units achterlaten, ligt dat anders. Hoewel elk afzonderlijk 'berichtje' geen problemen oplevert – een zeker voertuig A reed op moment t op locatie x – zou het wel een probleem zijn als alle meldingen van een coöperatief voertuig worden afgevangen en op een kaart geprojecteerd: er tekent zich dan een route af. Dat zou inzicht geven in het verplaatsingsgedrag van afzonderlijke voertuigen (en daarmee: van de gebruiker/bestuurder).

Het risico hierop lijkt niet heel groot, maar het coöperatieve systeem van Spookfiles A58 is al voorbereid op stevige maatregelen die dat probleem tackelen. Zo beschikken de on-board units over verschillende digitale identiteiten om berichten te ondertekenen. Het gebruik van meerdere identiteiten maakt het voor derden veel lastiger om op basis van verzonden berichten een afzender te herkennen.

De on-board units kunnen elke vijf minuten hun unieke herkenning ("MAC-adres") laten veranderen, zodat ze nooit langer dan enkele minuten achtereen dezelfde identiteit uitzenden.[3] Ook het coöperatieve systeem zelf 'weet' dan niet welk identiteit bij welk voertuig hoort. Dat voorkomt weer het volgen van de on-board units zelf.

Hoe staat het met de privacy als er meer diensten beschikbaar komen op het coöperatieve systeem?

Dat zal per nieuwe toepassing bekeken moeten worden: welke (nieuwe) data wordt er ingewonnen, opgeslagen en gedeeld en in hoeverre is dat een (nieuw) privacyrisico? Met het huidige systeem van data veilig opslaan en data aggregeren is al een stevige basis voor bescherming van de privacy gelegd. Ook is het coöperatieve systeem al voorbereid op het

[3] Veel apparaten hebben een vast MAC-adres, maar de on-board units niet. Dat heeft alles te maken met de gebruikte communicatietechnologie, wifi-p, die uitgaat van 'connectieloos communiceren'. Er wordt dus niet zoals bij GSM een verbinding gemaakt (daar is ook te veel tijd mee gemoeid): er worden alleen berichten uitgezonden. Dan kan er ook gemakkelijk van ID worden gewisseld.

verwijderen van de kop en staart van de ritten en het wisselen van MAC-adressen, wat de privacybescherming nog flink opschroeft.

Veiligheids- en privacymaatregelen volgens Europese standaarden

Alle (data)veiligheids- en privacy-maatregelen die in het Spookfiles A58-project worden toegepast, passen binnen Europese kaders zoals die vastgesteld zijn door ETSI, de European Telecommunications Standards Institute. In het project Spookfiles A58 zijn dus niet zozeer nieuwe concepten uitgedacht, maar zijn bestaande concepten *naar de praktijk vertaald*. Hierbij is belangrijke kennis en ervaring opgedaan: veel van de concepten werden niet eerder op zo'n grote schaal toegepast.

Het aansluiten op bestaande concepten en afspraken is natuurlijk belangrijk met het oog op de toekomst. Als er extra maatregelen op gebied van security en privacy nodig zijn omdat er ook uitgebreidere toepassingen komen, hoeft het veiligheids- en privacysysteem van Spookfiles A58 niet volledig te worden aangepast. Het bestaande systeem kan dan simpelweg worden uitgebreid.

24 mei 2016

Meer informatie: Trudy van de Westelaken, communicatieadviseur project Spookfiles A58: info@spookfiles.nl.