Slimme oplossingen voor veiligheids- en privacy-issues

Data zijn de drijvende kracht achter intelligente transportsystemen. Maar waar data worden gebruikt, loert het gevaar van lekken, stiekem meekijken en het ongeautoriseerd aanpassen van gegevens – de bekende (data) veiligheids- en privacy-issues. Om die reden werken de partijen in het project Spookfiles A58 niet alleen aan vernieuwende ITS, maar ook aan oplossingen voor de bijbehorende dataproblemen.

Spookfiles A58 is een van de projecten binnen het programma Beter Benutten van het Ministerie van Infrastructuur en Milieu. Bedrijven, overheid en kennisinstellingen werken hierin samen aan de introductie van een coöperatief systeem (wifi-p infrastructuur), met de A58 tussen Tilburg en Eindhoven als proeftraject. De eerste dienst die op het systeem draait, is de spookfiledienst: op basis van nauwkeurige informatie over stremmingen en filegolven op het proeftraject krijgen deelnemers vanuit de wegkant gepersonaliseerde *in-car* snelheidsadviezen toegezonden.

Wil het coöperatieve systeem zo'n advies kunnen genereren, dan moeten er wel heel wat gegevens verzameld, opgeslagen, bewerkt en verzonden worden. Het gaat daarbij om zowel 'publieke' data, zoals verkeersinformatie en de uiteindelijke adviezen die het systeem uitzendt, als om 'persoonsgebonden' data over de coöperatieve voertuigen, zoals hun exacte locatie, snelheid en richting. Het werken met deze data zal al snel leiden tot twee typen risico's: mogelijke problemen op het gebied van *(data)veiligheid* en issues met de *privacy*. Voor beide categorieën hebben de Spookfiles A58-partijen interessante oplossingen uitgewerkt die de risico's tot een aanvaardbaar niveau terugbrengen.*

(DATA)VEILIGHEID

Risico's

Onder (data)veiligheid vallen allereerst problemen met de ***beschikbaarheid.*** Doet de dienst het wel als de afnemer die wil gebruiken? Of doet er zich ergens in de keten een probleem voor met het inwinnen of delen van gegevens en leidt dat tot 'uitval' van de dienst? Ten tweede is er de ***authenticiteit*** van data. Kan de afnemer van een in-car service erop vertrouwen dat de informatie op het scherm van zijn device echt afkomstig is van de serviceprovider? En dan zijn er nog de zorgen om de ***integriteit***. Is het advies dat op het schermpje verschijnt juist? Is er niet bewust of onbewust iets aan de data veranderd?

Op zich zijn deze veiligheidsrisico's voor specifiek het project Spookfiles A58 klein: de spookfiledienst die wordt aangeboden is slechts een adviesdienst. Het ergste wat er kan gebeuren is dat er even géén advies binnenkomt of dat er een verkeerd advies op het scherm van het in-car device verschijnt (een advies om snelheid te minderen terwijl dat niet nodig is bijvoorbeeld). In beide gevallen zit de bestuurder 'ertussen' en die zal altijd zijn eigen beslissing nemen.

Maar omdat Spookfiles A58 een ontwikkel- en proefproject is, is besloten om toch stevige (data)beveiligingsmaatregelen te treffen. Dat is een mooie oefening voor toekomstige diensten waarbij de risico's wél groter zijn.

Oplossingen

Hoe worden de risico's rond ***beschikbaarheid*** getackeld? Dat is vooral een kwestie van kwaliteitscomponenten gebruiken, systemen en verbindingen redundant uitvoeren en de juiste (commerciële) *service level agreements* afsluiten. Het Spookfiles A58-systeem draait bijvoorbeeld op servers met een hoge gegarandeerde beschikbaarheid, geleverd door gespecialiseerde marktpartijen.

Het waarborgen van specifiek de ***integriteit*** en ***authenticiteit*** had meer voeten in aarde. Het projectteam heeft hiervoor een *Public Key Infrastructure (PKI)*-oplossing uitgewerkt.

PKI werkt kort gezegd als volgt. Elk systeem in Spookfiles A58 dat draadloos berichten verzendt – dat zijn de wegkantstations en de *on-board units* in de coöperatieve voertuigen – krijgt twee typen digitale 'sleutels': geheime sleutels waar alleen zij bij kunnen en een publieke sleutel die via een database voor iedereen toegankelijk is. De uitgifte en registratie van de sleutelsets worden streng bewaakt. 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 voertuig dit snelheidsadvies oppikt, zal het de ***publieke sleutel*** van het zendende station 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 hij beweert te zijn) en matcht die met de inhoud van het bericht? Komt er een 'OK' terug, dan weet het voertuig dat zowel de authenticiteit als de integriteit in orde zijn. Komt er een 'false' terug, dan is óf de verzender niet wie hij beweert te zijn of is het bericht gewijzigd.

PRIVACY

Risico's

Dan de privacy. Een eerste risico is dat er gedetailleerde data worden verzameld en opgeslagen van afzonderlijke (tot op individuen te herleiden) voertuigen. Bepaalde informatie wordt daarnaast gedeeld met derden. Dat roept vragen op: kunnen er geen onbevoegden bij de opgeslagen data? En wordt er geen privacygevoelige informatie gedeeld?

Een privacyrisico van een heel andere orde is het afvangen van data die coöperatieve voertuigen uitzenden. Hoewel een los 'berichtje' geen gevaar vormt – een zeker voertuig *A* reed op moment *t* op locatie *x* – is er wel een probleem als álle meldingen van een voertuig zouden worden afgevangen. Als iemand die op een kaart zou projecteren, tekent zich immers een route af. Dat zou inzicht geven in het verplaatsingsgedrag van afzonderlijke voertuigen (en daarmee: van de gebruiker/bestuurder).

Oplossingen

Welke oplossingen zijn op dit vlak uitgewerkt of in voorbereiding? Alle brondata die voor het project Spookfiles A58 worden verzameld, worden opgeslagen op de al genoemde servers. Die zijn niet alleen goed beveiligd tegen uitval, maar worden ook fysiek en digitaal stringent beveiligd.
De brondata, met daarin gegevens die tot op specifieke voertuigen zijn te herleiden, worden ook nooit zomaar overgedragen aan derden. Als er gegevens worden gedeeld – de coöperatieve data zijn vanuit verkeerskundig oogpunt erg waardevol – dan betreft dat altijd *geaggregeerde* data. De derde partij zal dus niet kunnen inzoomen op gegevens van afzonderlijke voertuigen. Een extra maatregel op dit vlak is 'in voorbereiding' en kan in een later stadium worden doorgevoerd: het verwijderen van de kop en staart van alle ritten. De begin- en eindpunten zijn namelijk moeilijker te aggregeren en om te voorkomen dat er dan toch informatie over afzonderlijke ritten wordt gedeeld, kunnen de laatste paar honderd meter van elke rit worden weggeknipt.[**]

Dan nog het punt dat alle berichten in theorie zijn af te vangen en mee te lezen. Is het een optie om de berichten die coöperatieve voertuigen uitzenden te versleutelen? Nee, want de kern van het cooperatieve systeem is samenwerken en het vrij delen van gegevens tussen de verschillende componenten (de voertuigen onderling, voertuig en wegkant).
Eén aanpak die is voorbereid, is dat de coöperatieve voertuigen de beschikking krijgen over meerdere digitale handtekeningen om de berichten mee te ondertekenen. Dit maakt het voor luistervinken veel lastiger om een zender te volgen op basis van ontvangen berichten.
Als extra zullen de *on-board units* in de coöperatieve voertuigen straks elke vijf minuten hun MAC-adres veranderen, zodat ze nooit langer dan enkele minuten dezelfde ID uitzenden.[***] Zelfs het coöperatieve systeem 'weet' dan niet welke ID bij welk voertuig hoort.

Tot slot

Spookfiles A58 heeft mooi werk geleverd voor de databeveiliging en privacybescherming van ITS-systemen. De oplossingen zijn allereerst voor het coöperatieve systeem op de A58 zelf: ze zijn al geïmplementeerd of in de architectuur is rekening gehouden met de implementatie ervan. Maar de oplossingen zijn zeker ook geschikt voor andere systemen, coöperatief of niet. Bij het uitwerken van de maatregelen hebben de Spookfiles A58-partijen zich namelijk keurig gevoegd naar de Europese kaders zoals die vastgesteld zijn door ETSI, de European Telecommunications Standards Institute. De oplossingen zijn in die zin ook niet nieuw. Wel is het voor eerst dat technieken als PKI in de coöperatieve praktijk op zo'n grote schaal worden toegepast. Het project heeft hiermee een stevige (data)veiligheids- en privacybasis gelegd voor de toekomst ●

* *Er bestaat niet zoiets als 100% (data)veiligheid of privacy, net zomin als een huis ooit 100% inbraakveilig zal zijn. Het doel van maatregelen is dan ook om risico's tot een aanvaardbaar niveau terug te dringen. Wat aanvaardbaar is zal van toepassing tot toepassing verschillen.*

** *Dit betekent dat er dan ook geen herkomst- en bestemmings-matrices uit de coöperatieve data te destilleren zijn, maar dat is de prijs die voor privacy betaald moet worden.*

*** *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.*

De auteurs

Peter Goossens *is chief technology officer bij Vialis.*
Willem de Boer *is security domain architect bij Technolution.*
Ir. Oene Kerstjens *is projectmanager Spookfiles A58*