Kilometerheffing op basis van elektronische aangifte

Betere fraude-bestendigheid en privacybescherming

Kilometerheffing is een doeltreffend beleidsinstrument dat – mede door Europese ontwikkelingen – ongetwijfeld weer op de politieke agenda komt. De auteur belicht de fraudebestendigheid en privacygevoeligheid van positie-gebaseerde kilometerheffingssystemen en pleit voor een aanpak gebaseerd op aangifte.

Wiebren de Jonge

Het is politiek verstandig om – als kilometer-heffing weer (meer) in beeld komt – in eerste instantie aan te sturen op een zogenoemde 'platte' heffing, waarbij voor een bepaald voer-tuig een vast bedrag per kilometer geldt. Het waarom hiervan vormt een verhaal op zich en valt buiten het bestek van dit stuk. Toch moet een te kiezen kilometerheffingssysteem vanwege de gewenste 'toekomstvastheid' ook tijd- en plaatsafhankelijke tarieven kunnen ondersteu-nen. Immers, zulke tarieven kunnen vroeg of laat toch nodig zijn. Hoe dan ook, het is duidelijk dat positiebepalingssystemen een rol zullen spelen.

Positiegebaseerde systemen

Onder positiegebaseerde kilometerheffingssyste-men verstaan we systemen waarbij ofwel de heffingsinstantie buiten de voertuigen hun posities bepaalt en bijhoudt, ofwel in de betrok-ken voertuigen een beveiligd kastje van of namens de heffingsinstantie wordt geplaatst dat continu positiegegevens ontvangt of zelf continu zijn – absolute – positie bepaalt.
In het eerste geval is er duidelijk sprake van een 'volgsysteem'. In het tweede geval is er sprake van een 'potentieel traceersysteem', omdat het beveiligde kastje dan in potentie heimelijk positiegegevens kan doorspelen naar (het deel van) de heffingsinstantie buiten de voertuigen. Immers, dat kastje heeft een communicatieka-naal nodig voor contact met de buitenwereld. Bijvoorbeeld om heffingstellerstanden bekend te kunnen maken aan de heffingsinstantie en/of om efficiënte controles mogelijk te maken. En dat toegestane communicatiekanaal kan altijd misbruikt worden als 'covert channel', dat wil zeggen voor het ongemerkt (!) overzenden van allerlei extra informatie. Bijvoorbeeld door gebruik te maken van geheime afspraken betref-fende de timing van de communicatie.

Privacy

Uit het oogpunt van privacybescherming is het ongewenst om de heffingsinstantie de mogelijk-heid te geven om uitgebreid informatie te verza-melen over op welke plaatsen een bepaald voertuig zich op welke tijdstippen heeft bevon-den. Volgsystemen zijn daarom evident onwen-selijk en positiebepaling vanuit een cellulair netwerk is dus geen goede optie. Maar ook

Samenvatting

Issues bij kilometerheffingssytemen zijn fraudebestendigheid en privacygevoeligheid. Volgens de auteur bedreigen zogenoemde positiegebaseerde systemen de privacy, maar kan de privacy wel goed gewaarborgd worden als de mobilist zelf controle heeft over het verzamelen en bijhouden van de benodigde informatie. Hij pleit daarom voor een aanpak waarbij apparatuur van de mobilist continu aangifte doet en waarbij de heffingsinstantie de juistheid van aangiften steekproefsgewijs en bij verrassing controleert. Zo'n aanpak heeft ook grote voordelen voor de fraudebestendigheid en de kosten.

positiegebaseerde heffingssystemen van het andere type leveren, zoals hierboven is geschetst, een serieus gevaar op voor de privacy. Merk op dat het weinig zin heeft om in een wet vast te leggen dat het kastje geen positiegegevens mag verzamelen en overseinen naar buiten het voertuig, omdat niet goed te controleren valt of men zich aan zo'n wet houdt. Kortom, een vuistregel is dat de privacy alleen wordt gewaarborgd als het kastje van de heffingsinstantie helemaal geen positiegegevens of andere privacygevoelige gegevens verstrekt krijgt.

Fraude

Een heffingssysteem moet beveiligd worden tegen allerlei fraudemogelijkheden. Dat kan met fysieke maatregelen, maar ook met maatregelen op een logisch niveau, zoals juridische, organisatorische en procedurele maatregelen. Denk bij fysieke beveiliging aan het zodanig fysiek uitvoeren van het systeem dat een poging tot fraude moeilijker wordt. Een bankkluis is bijvoorbeeld fysiek zodanig uitgevoerd dat het moeilijker is om er geld uit te halen of om hem in z'n geheel mee te nemen dan in geval van een sigarenkistje of de eerste de beste kassa.
Alle andere beveiligingsmaatregelen vallen onder de noemer van logische beveiliging. In deze context is de belangrijkste vorm de combinatie van efficiënte fraudedetectie en juridische maatregelen (strafwetten). Reële kans op ontdekking en straf maakt fraude minder aantrekkelijk en draagt dus indirect bij aan de fraudebestendigheid.

Kosten

Omdat elke fysieke beveiligingsmaatregel doorbroken kan worden, is er bij fysieke beveiliging altijd sprake van een 'wapenwedloop'. Elke maatregel leidt tot een tegenmaatregel, die weer leidt tot een tegen-tegenmaatregel, enzovoorts. Samen met de 'wet van de verminderde meeropbrengst' leidt dit in het algemeen tot aanzienlijke kosten. Hier komt bovenop dat het beveiligingsniveau bepaald wordt door de zwakste schakel en dat dure fysieke inspecties nodig zijn om te controleren of een fysieke maatregel niet doorbroken is. Het op willekeurige tijdstippen en plaatsen uitvoeren van visuele inspecties op de heffingsapparatuur van passerende voertuigen is niet alleen duur, maar ook nog eens slecht voor de doorstroming van het verkeer, omdat men de voertuigen eerst moet aanhouden. Kortom, de noodzaak tot fysieke beveiliging kan maar beter geminimaliseerd worden en steekproefsgewijze controles moeten bij voorkeur zonder verkeershinder en dus op afstand kunnen worden uitgevoerd.

Controles

Controles uitvoeren op enige afstand van passerende voertuigen via telecommunicatie met heffingsapparatuur in die voertuigen biedt een aantal belangrijke voordelen boven fysieke inspecties. Ten eerste zijn zulke controles veel goedkoper en dus efficiënter, omdat ze beter te automatiseren zijn en minder personeel vereisen (o.a. geen aanhouding nodig). Door de lagere kosten kunnen ze veel intensiever plaatsvinden, zodat elk voertuig gemiddeld vele keren per jaar gecontroleerd wordt in plaats van slechts een enkele keer, zoals bijvoorbeeld bij de APK. Ten tweede zijn zulke controles veel effectiever. Enerzijds omdat ze zonder hinder voor het verkeer uitgevoerd kunnen worden, zodat de heffingsapparatuur in het voertuig op goede werking gecontroleerd kan worden tijdens verkeersdeelname en dus terwijl de heffingsapparatuur in bedrijf is. Anderzijds omdat ze veel beter op verrassende plaatsen en tijdstippen kunnen worden uitgevoerd. Immers, een groter verrassingseffect verbetert de effectiviteit. Kort-

om, verrassingscontroles tijdens verkeersdeelname zijn veel effectiever tegen fraude dan controles op geplande momenten in een werkplaats, zoals bijvoorbeeld bij de APK.
Ten slotte is er nog een belangrijk aspect: er kunnen meer dure – en toch altijd doorbreekbare – fysieke beveiligingsmaatregelen vervangen worden door steekproefsgewijze controles (i.e., fraudedetectie en straffen) naarmate zulke controles beter, goedkoper en met meer verrassing kunnen worden uitgevoerd.

Elektronische aangifte

In 1998 ontstond het idee van zogenoemde aangiftegebaseerde systemen[1]. Fysieke beveiliging is hierbij niet of nauwelijks van cruciaal belang. De betrokken mobilisten moeten vrijwel continu aangifte doen en zijn zelf verantwoordelijk voor, en hebben ook zelf controle over, het verzamelen en bijhouden van de benodigde informatie. Natuurlijk hoeven mobilisten niet zelf na elke afgelegde meter handmatig een formuliertje in te vullen, maar zorgt apparatuur in het voertuig steeds voor het automatisch samenstellen en indienen van een elektronische aangifte namens de mobilist. Elke aangifte moet bepaalde informatie omvatten, zoals bijvoorbeeld de huidige stand van de heffingsteller.

De heffingsinstantie controleert de in of vanuit voertuigen beschikbaar gestelde aangiften steekproefsgewijs en bij verrassing (zie verderop). De controles kunnen tijdens verkeersdeelname (dus effectief en zonder aanhouding) vanaf enige afstand (dus zonder verkeershinder) via telecommunicatie (dus efficiënt) worden uitgevoerd. Omdat de mobilist zelf controle heeft over de actuele inhoud van zijn of haar aangiften, kan er niet heimelijk privacygevoelige informatie in worden verstopt, zoals informatie over alle plaatsen waar het voertuig op welke tijdstippen is geweest. Door gepast gebruik van encryptie is elk gegeven uit een aangifte alleen leesbaar voor de juiste bevoegde instantie.

Beschikbaarstelling

Een essentieel element van bovengemelde aanpak is dat vrijwel continu (bijvoorbeeld enkele malen per seconde) aangiften moeten worden samengesteld en dat de heffingsinstantie op elk door haar gekozen moment toegang moet kunnen krijgen tot de stroom van aangiften. Er zijn twee manieren waarop dit bereikt kan worden.
Ten eerste door de aangiften naar een in het voertuig aanwezige chip van de instantie te sturen. Deze chip fungeert als een beveiligde brievenbus die alleen de laatste aangiften vasthoudt, bijvoorbeeld die van de laatste paar kilometer. Alleen de heffingsinstantie kan via ('request-response') telecommunicatie toegang krijgen tot deze aangiften. Een indiener kan een eenmaal gedane aangifte dus niet uit deze brievenbus terughalen. Hij kan dus niet een valse aangifte terugnemen om die nog gauw even te corrigeren als zijn voertuig een 'request' ontvangt (en hij kan vermoeden dat hij gecontroleerd gaat worden). In deze variant is uitsluitend de fysieke beveiliging van de in de chip opgeslagen informatie van cruciaal belang.
Een tweede, qua beveiliging minstens zo interessante manier is om de aangiften continu naar buiten te laten zenden via een zender met een bereik van enige tientallen meters, zeg 50 tot 100 meter. Op elke willekeurig gekozen plaats en tijdstip kan de heffingsinstantie dan met een ontvanger de door passerende voertuigen uitgezonden aangiften onopgemerkt opvangen.
Slechts een fractie van alle uitgezonden aangiften komt dus werkelijk bij de heffingsinstantie terecht. Bij deze tweede variant met continue transmissie is geen enkele fysieke beveiligingsmaatregel strikt noodzakelijk, omdat men desgewenst elk beveiligingsniveau kan bereiken uit-

1. W. de Jonge (2001). Systemen voor fraudebestendige en privacyvriendelijke kilometerheffing. Rapport IR-487. Faculteit Exacte Wetenschappen, Vrije Universiteit. (PDF-versie op: www.cs.vu.nl/~wiebren)

sluitend met steekproefsgewijze verrassingscontroles.
In het navolgende gaan we in op een aantal aspecten van deze tweede variant. Voor meer informatie over de eerste variant verwijzen we naar het al eerder aangehaalde rapport[1].

Controles

Een goede controle bestaat uit het doen van onafhankelijke metingen en/of waarnemingen bij het gecontroleerde voertuig en het vergelijken van de verkregen resultaten met de corresponderende aangifte(n).
Bij kilometerheffing moet vooral gecontroleerd worden of de tellerstand correct wordt opgehoogd. Dat kan bijvoorbeeld door de uitgezonden heffingstellerstand op twee opeenvolgende punten langs een weg te onderscheppen en te controleren of het verschil tussen die twee standen overeenstemt met het correcte bedrag verschuldigd voor dat voertuig op die afstand tussen die twee punten. Of men kan een meting van de snelheid van een passerend voertuig gebruiken om de correcte, gewenste toenamesnelheid van zijn heffingstellerstand te bepalen en die dan vergelijken met de toenamesnelheid van de heffingsteller volgens de op hetzelfde tijdstip onderschepte aangifte(n). Een voordeel van een controle met onderschepping op één moment (en gebruikmaking van eerste afgeleiden) is dat er niet per se gebruik hoeft te worden gemaakt van een – leesbare – identificatie in de aangifte, wat de privacybescherming ten goede kan komen. Kortom, er kan vrij makkelijk gecontroleerd worden of een tellerstand op een bepaald moment of traject correct wordt bijgehouden. Zolang de mobilist maar niet weet welke aangiften wel en welke niet gecontroleerd worden, is hij of zij min of meer gedwongen steeds correct aangifte te (laten) doen. Althans, zolang ervoor gezorgd wordt dat de kans op controle (en dus op ontdekking van een poging tot fraude) maal de hoogte van de boete voldoende hoog is.

Verrassingseffect

Alleen het gebruik van continue transmissie maakt goede en effectieve verrassingscontroles mogelijk. Immers, bij de tot nu toe gebruikelijke 'request-response' communicatie geeft een controlepost bij de eerste de beste controle zijn positie al prijs door een 'request' naar het te controleren voertuig te zenden. In de nabije toekomst kan elk voertuig dat een dergelijk 'request' ontvangt onmiddellijk, via een snel netwerk alle andere voertuigen informeren over de plaats waar hij de 'request' ontvangen heeft en waar dus ogenschijnlijk gecontroleerd wordt. Het verrassingseffect kan aldus in hoge mate weggenomen worden, zelfs van mobiele controles vanuit patrouillewagens.
Bijvoorbeeld kan een navigatiesysteem geheel automatisch alternatieve routes uitrekenen waarbij een geschat risicogebied rondom de plaats van recente controles gemeden wordt. Of een fraudeur zorgt ervoor dat zijn apparatuur in de risicogebieden wel goed werkt. Effectief bij verrassing controleren wordt dan veel duurder, omdat men zich na elke controle weer moet verplaatsen en moet wachten tot het geschatte gebied voldoende is 'uitgedijd' om een volgende controle voldoende verrassingseffect te geven.

»Verrassingscontroles tijdens verkeersdeelname zijn het effectiefst«

Optimale mix

Bij deze aanpak zijn alle componenten (zoals bijvoorbeeld zender, positiebepalingssysteem, display en sensors) slechts hulpmiddelen. Omdat deze hulpmiddelen onder verantwoordelijkheid van de aangifteplichtige functioneren, is fysieke beveiliging ervan niet per se noodzakelijk.
Om de intensiteit – en dus kosten – van controle te kunnen verlagen, kan het voordelig zijn bepaalde fysieke beveiligingsmaatregelen aan te brengen. Omdat deze slechts bedoeld zijn tegen de meest simpele fraudepogingen en ze niet cruciaal zijn voor de fraudebestendigheid, kan men zich hierbij probleemloos beperken tot relatief simpele maatregelen met een prima prijs-prestatieverhouding. Kortom, de apparatuurkosten kunnen desgewenst relatief laag gehouden worden.
Omdat bij de aanpak met continue transmissie alle fysieke beveiliging inwisselbaar is met logische beveiliging, kan men voor het bereiken van een gewenst niveau van fraudebestendigheid kiezen voor een optimale mix van beide vormen. De mix met de beste prijs-prestatieverhouding zal ongetwijfeld ergens tussen de twee uitersten van uitsluitend fysieke of uitsluitend logische beveiliging in liggen.

Naast het kostenaspect is van groot belang dat toekomstige doorbreking van een fysieke maatregel soepel opgevangen kan worden. Een onverwacht slimmigheidje of nieuwe technische mogelijkheden hoeven dus nooit fataal te zijn. Immers, zodra ontdekt wordt dat doorbreking mogelijk is, kan men de controle-intensiteit (de logische beveiliging) tijdelijk opvoeren om het gewenste beveiligingsniveau te handhaven. Er is dan alle tijd om betere fysieke beveiliging te ontwerpen en aan te brengen, alvorens de intensiteit van de controles weer terug te brengen naar een optimum.
Dit is een niet te onderschatten voordeel boven alle andere systemen, waarbij niet alle fysieke beveiliging vervangen kan worden door logische. Als bij zo'n ander systeem een cruciale fysieke beveiligingsmaatregel doorbroken wordt, dan dreigt dat systeem 'in te storten'. Anders gezegd, dan kan de inkomstenstroom gedurende langere tijd aanzienlijk afnemen of zelfs opdrogen, simpelweg omdat het ontwerpen en het aanbrengen in miljoenen voertuigen van fysieke wijzigingen al gauw enkele jaren vergt en het beveiligingslek dus niet snel gedicht kan worden.
Kortom, continue transmissie maakt volledige uitwisselbaarheid van logische en fysieke beveiliging mogelijk en levert daarmee niet alleen een belangrijke bijdrage aan het laag houden van de initiële en operationele kosten, maar ook aan grotere flexibiliteit en aan betere (waaronder ook toekomstvastere) fraudebestendigheid.

Ten slotte

Bovenstaande is slechts een grove, maar hopelijk wel voldoende schets van het belang van uitwisselbaarheid van logische en fysieke beveiliging, van 'toekomstvastheid' van de fraudebestendigheid, van continue transmissie voor het gewenste verrassingseffect van controles, en een schets van het gevaar voor de privacy van zogenoemde positiegebaseerde systemen.
Er is geen enkel bezwaar tegen het gebruik van een GPS-ontvanger of een ander systeem voor positiebepaling, ook niet voor kilometerheffing. Althans, niet als de mobilist de mogelijkheid krijgt om desgewenst te zien wat er met de positiegegevens gebeurt. Echter, als de positiegegevens terechtkomen in een kastje dat fysiek beveiligd is tegen toegang door de mobilist, dan is zulks zeker niet het geval. Hij of zij kan dan niet controleren of er misschien in het kastje heimelijk toch privacybedreigende informatie over afgelegde routes wordt bijgehouden die naar buiten kan worden 'gelekt' via een verborgen kanaal. Dit zou een serieus bezwaar kunnen zijn tegen het (toekomstige) gebruik van positiegebaseerde kilometerheffingssystemen.

»Continue transmissie vergroot de mogelijkheden voor verrassing«

Het in de privacywetgeving opgenomen subsidiariteitsbeginsel houdt min of meer in dat de overheid een doel op de minst privacybelastende wijze moet verwezenlijken die in redelijkheid mogelijk is. Omdat bij aangiftegebaseerde systemen zulke 'lekkage' veel beter voorkomen kan worden, kan men geneigd zijn te concluderen dat een positiegebaseerd kilometerheffingssysteem niet in aanmerking komt.
Echter, zo eenvoudig liggen de zaken allerminst. Op Europees niveau wordt hard gewerkt aan richtlijnen[2] voor verkeersheffingssystemen, die het gebruik van GPS in een beveiligd kastje van een instantie allerminst uitsluiten en die bepaalde privacyvriendelijkere oplossingen zelfs – onbedoeld en/of ongemerkt – onmogelijk kunnen maken. (Bijvoorbeeld door een ongelukkige keuze van welke soorten of vormen van communicatietechnologie toegestaan of verplicht worden.) Er kan mijns inziens alleen voorkomen worden dat 'we' over vele jaren via de Europese route mogelijk een door Nederland(ers) niet gewenst systeem 'opgedrongen' krijgen, als Nederland spoedig de diverse alternatieven gaat onderzoeken en op dit punt zijn invloed meer gaat aanwenden.

Wiebren de Jonge
is universitair hoofddocent bij de afdeling Informatica van de Faculteit Exacte Wetenschappen van de Vrije Universiteit te Amsterdam (0,8 fte) en dga van TIP Systems B.V. E-mail: wiebren@cs.vu.nl.

2. COM (2003) 132 final, Brussels, 23.04.2003 - 2003/0081 (COD): communication from the Commission: developing the trans-European transport network: innovative funding solutions - interoperability of electronic toll collection systems: proposal for a directive of the European Parliament and of the Council on the widespread introduction and interoperability of electronic road toll systems in the Community.