Aan
de voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Contactpersoon
-
Datum
14 april 2008
Ons kenmerk
VENW/DGP-2008/3843
Onderwerp
"OV-chipkaart "Counter expertise"

Doorkiesnummer
-
Bijlage(n)
2
Uw kenmerk
-

Geachte voorzitter,

Hierbij bied ik u de "OV-chipkaart counter expertise" van de "Royal Holloway University of London" (RHUL) aan. Ik stuur u de Engelse originele rapportage en de Nederlandse vertaling hiervan[1].

Deze contra-expertise op het TNO-onderzoek naar de beveiliging van de OV-chipkaart is in mijn opdracht uitgevoerd. Tijdens het debat van 17 januari 2008 heb ik deze contra-expertise aangekondigd. Het doel van de contra-expertise is te beoordelen of het in opdracht van TransLink Systems (TLS) uitgevoerde TNO-onderzoek methodologisch juist is uitgevoerd, of het onderzoek volledig is en of de conclusies en voorstellen goed gefundeerd, juist en eenduidig zijn.

Beoordeling van het TNO-Onderzoek
De RHUL stelt dat TNO methodologisch goed te werk is gegaan en heeft twee hoofdpunten van kritiek:

[1] Dit document bevat de vertaling van het in het Engels gepubliceerde rapport *Counter Expertise Review of the TNO Security Analysis of the Dutch OV-Chipkaart*, uitgebracht door Royal Holloway University of London (RHUL) aan het Ministerie VenW. In deze vertaling is de inhoud en strekking van het oorspronkelijke rapport zo nauwkeurig mogelijk benaderd, zodat het Nederlandse parlement en publiek hiervan zonder taalbarrière kennis kunnen nemen. Om echter discussie over mogelijke interpretatie- en nuanceverschillen te voorkomen, blijft het originele Engelse eindrapport van de RHUL het enige met formele status. Hoewel aan de vertaling zowel inhoudelijk als tijdens de totstandkoming uiterste zorg is besteed, aanvaardt het ministerie geen aansprakelijkheid voor eventuele fouten en onvolkomenheden, noch voor de gevolgen hiervan.

Postadres Postbus 20901, 2500 EX Den Haag
Bezoekadres Plesmanweg 1-6, 2597 JG Den Haag
Telefoon 070 351 61 71
Fax 070 351 78 95

- De RHUL constateert dat TNO teveel is uitgegaan van de huidige stand van de techniek om toekomstige aanvallen goed in te schatten. Er zijn inmiddels andere 'aanvalsmethoden' bekend, die goedkoper, sneller en simpeler kopiëren of veranderen van de kaart mogelijk maken. TNO heeft deze conclusie inmiddels zelf ook getrokken na aanvullend onderzoek (gepubliceerd eind maart 2008).
- De RHUL constateert dat TNO daarnaast is uitgegaan van de huidige omvang van het systeem (pilots Rotterdam/Amsterdam/NS), en heeft daarmee geen rekening gehouden met de toekomstige financiële waarde in het systeem bij nationale uitrol.

Conclusies/aanbevelingen
Het RHUL-rapport bevat een veelheid aan conclusies en aanbevelingen, die komen op het volgende neer:

- De RHUL concludeert met TNO: "er is sprake van één heldere conclusie waarbij één boodschap als rode draad door het rapport heen loopt: de Mifare Classic-kaart moet worden vervangen".
- Volgens de RHUL zal een vervanger voor de Mifare Classic-kaart gebaseerd moeten zijn op een algoritme dat is getest door cryptografische experts (de 'cryptographic expert community'). De chip mag niet gebaseerd zijn op een geheim algoritme en dient voldoende lange veiligheidssleutels te bevatten.
- Daarnaast beveelt de RHUL aan om toekomstige OV-chipkaarten in elk geval één gezamenlijk en herkenbaar antifraudekenmerk te geven, bijvoorbeeld een lasergravure of een hologram, ten behoeve van fysieke kaartcontrole.
- De RHUL wijst er met grote nadruk op dat bij het ontwerpen, invoeren, exploiteren en verbeteren van dit soort systemen zeer strenge risico-beoordelingsmethodieken moeten worden toegepast. In het geval van het OV-chipkaartsysteem zouden volgens de RHUL alle momenteel gebruikte kaarttypes aan deze risico-beoordeling moeten worden onderworpen, inclusief de Mifare Ultralite.
- De RHUL constateert dat een criminele aanval zich kan richten op het kaartsaldo of opwaarderingen daarvan. Hoewel de kaarthouder deze schade vergoed krijgt, zal het overlast geven. De RHUL nuanceert dit door het volgende te stellen: "burgers lopen veel meer kans slachtoffer te worden van fraude en misbruik via algemene services via het internet of de telefoon".
- De RHUL onderschrijft de conclusie van TNO dat privacygegevens niet in het geding zijn, omdat de chip zelf alleen de geboortedatum en de laatste reisgegevens bevat.
- Ook geeft de RHUL aan dat op het moment dat sprake is van een landelijke uitrol de financiële omvang wellicht wel interessant is voor criminelen. Op dit moment is dat volgens RHUL nog niet het geval, gezien de omvang van de proef in Rotterdam en Amsterdam. De uitvoerbaarheid van de correctieve maatregelen die TNO heeft voorgesteld is volgens RHUL nog onvoldoende bewezen en dient met urgentie te worden onderzocht.
- De RHUL beveelt aan een migratieplan op te stellen, waarin alle noodzakelijke activiteiten, betrokken partijen, budgetten en technologie zijn omschreven. Hiertoe is het noodzakelijk dat gestructureerde risico-analyses gemaakt worden (voor alle kaartsoorten en -lezers) en er dienen voor mogelijke aanvallen tegenmaatregelen klaar te liggen. Wanneer de landelijke uitrol van de OV-

chipkaart een feit is, moeten TLS en de OV-bedrijven gereed staan om zo nodig het migratieplan en zo snel mogelijk uit te voeren.

Vervolg
Naar aanleiding van het rapport heb ik de volgende vragen gesteld aan TLS en de deelnemende OV-bedrijven:

- Is het bestaande noodplan nog adequaat nu en in de toekomst?
- Hoe ziet u, gelet op de conclusies en aanbevelingen van de RHUL, het vervolgtraject en de vervolgplanning?
- Wanneer kunt u een migratieplan opleveren?

De decentrale overheden hebben rondom de invoering van de OV-chipkaart een specifieke rol. Zij zijn als concessieverlener verantwoordelijk voor een zorgvuldige introductie via de vervoersconcessies. Ik heb aan hen de volgende vragen gesteld:

- Welke consequenties heeft dit rapport voor de invoering van de OV-chipkaart in uw concessiegebieden?
- Leiden deze conclusies wat u betreft tot aanpassingen van de bestuursovereenkomsten?

Zojuist heb ik TLS, de OV-bedrijven en de decentrale overheden de contra-expertise toegezonden. Ik hoop spoedig antwoorden te krijgen op de vragen die ik aan hen heb gesteld. Het is voor mij van groot belang helderheid te krijgen over de consequenties die partijen verbinden aan het rapport van de RHUL.

Zoals ik al eerder schreef, schaf ik het NVB pas af als ik ervan overtuigd ben dat de reiziger op de OV-chipkaart kan vertrouwen. Ik vraag mij in alle ernst af of de datum van 1 januari 2009 TLS, OV-bedrijven en decentrale overheden gelet op de uitkomsten van de rapportages van TNO en RHUL nog haalbaar is. Ook deze vraag heb ik aan de betrokken partijen voorgelegd.

Hoogachtend,

DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT,

J.C. Huizinga-Heringa