Beoordeling migratieplan voor de OV-chipkaart

06-01-10

Hoofdlijnen van het rapport

Op basis van de contra-expertise (CE) van het TNO-rapport over de beveiligingsproblemen van de Mifare Classic-kaart en de OV-chipkaart heeft de Information Security Group/Smart Card Centre (ISG/SCC) van Royal Holloway, University of London (RHUL) geadviseerd voorafgaand aan landelijke invoering van de OV-chipkaart een mijlpaal voor migratieplanning (MPM) vast te stellen. Het Nederlandse ministerie van Verkeer en Waterstaat (VenW) heeft Trans Link Systems (TLS) en de exploitanten van openbaar vervoer (PTO's [Public Transport Operators]) verzocht een gecontroleerd en goedgekeurd *migratieplan* gereed te hebben voordat de algemene verplichting om de papieren strippenkaart in het lokale en regionale openbaar vervoer in Nederland te accepteren, wordt opgeheven. VenW heeft RHUL verzocht een onafhankelijke beoordeling uit te voeren van de voor dit *migratieplan* gebruikte documentatie, en te bepalen of TLS en de PTO's op basis van een aantal door VenW vooraf gedefinieerde eisen, die zijn gericht op het bepalen van de technische en operationele gereedheid voor migratie, in voldoende mate gereed zijn om te migreren.

Uit de beoordeling van de technische gereedheid op basis van de geleverde documenten, komt het beeld naar voren dat de nieuwe kaarttechnologie een architectuur ondersteunt die ontworpen is voor flexibiliteit, voldoende toekomstbestendig is, en de afhankelijkheid van leverancierspecifieke implementaties vermindert. Voor het protocol wordt gebruikgemaakt van een openbaar algoritme met een sleutelformaat dat beantwoordt aan internationale aanbevelingen. Positieve aspecten zijn verder het gebruik van blokvercijfering in plaats van stroomvercijfering, wat een betere beveiliging biedt, en een extra beveiligingslaag in de vorm van gegevensauthenticatie. De prestaties van het systeem (in ieder geval aan de kant van de kaart) lijken voldoende te zijn voor de bedoelde toepassing. Op basis van deze bondige beoordeling heeft RHUL geen opvallende, grote gebreken gevonden in het ontwerp (voor het protocol en het kaartsysteem), hoewel natuurlijk van openbare beoordelingen bekend is dat de veiligheid met meer zekerheid kan worden vastgesteld naarmate er meer beoordelaars bij worden betrokken. TLS is daarom aangeraden meer zekerheid te verkrijgen over de veiligheid van het protocolontwerp en de uiteindelijke implementatie aan de hand van een 'open' benadering of door inschakeling van commerciële of universiteitslabs[1].

De keuze voor het SmartMX-kaartplatform van NXP is gebaseerd op beredeneerde argumenten, hoewel er vanwege de vereisten van TLS voor ondersteuning van het oude protocol (Mifare Classic) erg weinig alternatieven waren. Op de lange termijn (als ondersteuning van het oude systeem niet meer nodig is) is er tevens de mogelijkheid om gebruik te maken van algemene typen beveiligde microcontrollers. RHUL heeft vastgesteld dat de belangrijkste risico's met betrekking tot de verbeteringen in de infrastructuur zijn onderkend en dat voor elk van deze risico's als onderdeel van het algemene activiteitenplan een leveranciersplan is opgesteld. Hoewel technische gereedheid nog niet is bereikt, wordt verondersteld dat dit zal gebeuren als de geplande activiteiten zijn uitgevoerd.

Teneinde de operationele gereedheid vast te kunnen stellen, werd door TLS in eerste instantie een 'voorlopige' set documenten ter beoordeling geleverd. In de hierin opgenomen plannen werd echter een aantal leverancierstaken dubbel uitgevoerd en het besluitvormingsmodel voor het beginmoment van de migratie bevatte onduidelijkheden. Naar het oordeel van RHUL waren deze plannen dan ook ontoereikend om adequaat te kunnen reageren in het geval zich een bedreiging

[1] Uit gesprekken is naar voren gekomen dat er door TLS waarschijnlijk al met commerciële of universiteitslabs wordt gewerkt aan meer zekerheid betreffende de beveiliging.

zou voordoen die zich snel uitbreidde. TLS had ook vastgesteld dat er sneller gereageerd moest kunnen worden en leverde voor de verdere beoordeling een set definitieve documenten met aanzienlijke wijzigingen. De aangepaste strategie in de definitieve plannen is gebaseerd op het uitgangspunt dat er meteen met het migratieproces wordt begonnen, zodat de cruciale technische voorbereidingen zo snel mogelijk kunnen worden afgerond, en bepaalde inspanningen niet dubbel worden verricht. De migratie wordt geleidelijk uitgevoerd, tenzij er een grote bedreiging (fraude of aanval) wordt geconstateerd. In een dergelijk geval wordt de migratie versneld om de bedreiging snel genoeg het hoofd te kunnen bieden. Wanneer op 1 februari 2010 met de definitieve plannen wordt begonnen, kan op 1 november 2010 een 'gekwalificeerd' stadium van migratiegereedheid zijn bereikt. We noemen dit stadium gekwalificeerd, omdat voor het in werking treden van het versnelde plan een effectief besluitvormingsmodel (DFA) noodzakelijk is. Op grond van de herziene beoordelingsvereisten[2] van VenW heeft RHUL een aantal aanbevelingen gedaan voor verbetering van het DFA, die als volgt kunnen worden samengevat:

- het aantal triggervariabelen wordt uitgebreid met kwantiteiten die verband houden met acceptatie door de klant, de belasting van IT-systemen en kostengerelateerde kwesties;
- er worden modellen gedefinieerd waarmee potentiële escalatietrends voor triggervariabelen kunnen worden voorspeld;
- er wordt niet uitgegaan van landelijke gemiddelden, maar voor ieder netwerk en/of iedere PTO worden de triggervariabelen apart berekend;
- er wordt een volledige set aanvankelijke drempelwaarden voor triggers gedefinieerd;
- er wordt een procedure vastgelegd voor mogelijke aanpassing van de drempelwaarden voor triggers;
- in het DFA-document wordt een procedure opgenomen voor herzieningen van de migratieplannen en de bijbehorende documenten.

Ervan uitgaand dat de definitieve plannen worden uitgevoerd en dat TLS de aanbevelingen van RHUL voor het DFA binnen twee maanden na aanvang van de definitieve planning aanvaardt en overneemt, is de conclusie van RHUL dat TLS en de PTO's op 1 november 2010 gereed zouden moeten zijn voor migratie, als met de werkzaamheden wordt begonnen op 1 februari 2010.

[2] Deze herzieningen waren nodig omdat in de oorspronkelijke beoordelingscriteria geen rekening was gehouden met een versnelling van de migratie.