Institute for Computing and Information Sciences

Digital Security

Postadres:
Postbus 9010
6500 GL Nijmegen

Bezoekadres:
Huygensgebouw
Heyendaalseweg 135
6525 AJ Nijmegen

Telefoon: 024-3653133
Fax: 024-3652298

http://www.ru.nl/ds

Vaste commissie voor Verkeer en Waterstaat
Tweede Kamer der Staten Generaal
Postbus 20018
2500 EA Den Haag

Ons kenmerk	Uw kenmerk	Doorkiesnummer	Datum
08.011/WT		024-3652077	16 juni 2008

Betreft
Hoorzitting 18 juni a.s.

E-mail
w.teepe@cs.ru.nl

Geachte Leden van de Tweede- Kamercommissie Verkeer en Waterstaat,

Allereerst mijn dank voor uw uitnodiging voor de hoorzitting van 18 juni over de OV-chipkaart. Als lid van de Digital Security onderzoeksgroep van de Radboud Universiteit Nijmegen, neem ik deze uitnodiging graag aan. Via uw griffier heb ik informeel enkele vragen ontvangen die in de hoorzitting aan de orde zouden kunnen komen.

1. Wat zijn de risico's bij het verder ontwikkelen van deze kaart?
2. Hoe beoordelen jullie de veiligheidsmaatregelen (van de staatssecretaris)?
3. Hoe beoordelen jullie het rapport van de deskundigen uit Londen (de contra-expertise van Royal Holloway University of London (RHUL))?
4. Hoe beoordelen jullie het feit dat er blijkbaar bij de Oyster Card in Londen niet veel mis gaat?

Ik zal in de hoorzitting proberen deze, en eventuele andere, vragen zo goed mogelijk te beantwoorden. Ik maak graag van de gelegenheid gebruik om in deze brief vast enige zaken uiteen te zetten die mij van belang lijken bij de beantwoording van deze vragen.

Functionaliteit versus beveiliging
Allereerst is er het onderscheid tussen *functionaliteit* en *beveiliging*. Dit is het makkelijkste uit te leggen aan de hand van een eenvoudig voorbeeld.

Bij mij in de wijk is een kinderboerderij, met op het terras een tafel waarop consumpties staan zoals koffie, ranja en gevulde koeken. Ernaast staat een prijslijst en een (goed vastgemaakt) spaarvarken. De afspraak is dat wie een consumptie neemt, het verschuldigde bedrag in het spaarvarken stopt.

Dit primitieve betaalsysteem *functioneert* prima: vrijwel iedereen die een consumptie neemt betaalt deze. Bijzonder goed *beveiligd* is het systeem niet: het is relatief eenvoudig om een consumptie van de tafel te nemen en daar niet voor te betalen. Dat er niet op grote schaal misbruik wordt gemaakt van dit lek heeft te maken met dat de consumpties een beperkte waarde hebben, ze tegen een spotprijs worden aangeboden, en het publiek begrip heeft voor de krappe financiële kaders van een kinderboerderij.

Voor een betaalsysteem zoals de OV-chipkaart is het ook goed dit onderscheid tussen *functionaliteit* en *beveiliging* te maken. Zolang iedereen zich aan de afspraken houdt functioneert het prima: mensen betalen voor hun reizen en de vervoerders krijgen dit op hun rekening bijgeschreven. Dit is ook het geval bij de Oyster Card in Londen. De *beveiligings*complicatie die er sinds de recent gebleken kwetsbaarheden van de Mifare Classic is, is dat het mogelijk is om je als reiziger niet aan de afspraak te houden, en te reizen zonder daarvoor te betalen. Dat is conceptueel precies hetzelfde als bij de kinderboerderij een gevulde koek van de tafel pakken zonder daarvoor te betalen.

De nieuwe kennis over zwakheden in de Mifare Classic heeft voor de Oyster Card dezelfde gevolgen als voor de OV-chipkaart. Wanneer er software op het internet komt waarmee kaarten gekloond of bedragen teruggezet kunnen worden, heeft dit voor beide systemen dezelfde gevolgen. De Radboud Universiteit Nijmegen zal zelf zulke software niet verspreiden, maar het is redelijk (en verstandig) te verwachten dat er andere partijen zullen zijn die dit wel gaan doen. De beschikbaarheid van dergelijke software kan het mogelijk maken dat ook leken misbruik kunnen maken van de zwakheden in de beveiliging.

Het is op zijn plaats om te melden dat er in onze onderzoeksgroep aan de Radboud Universiteit Nijmegen vooral beveiligingsexpertise aanwezig is, en niet zozeer expertise over risicoanalyse: het met onderbouwde cijfers voorspellen hoeveel fraude er in de specifieke OV-chipkaart casus te verwachten is. Voor een verstandig besluit is een dergelijke risicoanalyse noodzakelijk, en daarvoor zullen experts op dit gebied geconsulteerd moeten worden. Wij beperken ons tot ons vakgebied en hebben daarbinnen een duidelijke waarschuwing afgegeven.

Scenario's

Vervolgens zijn er een aantal wezenlijk verschillende scenario's voor het verder ontwikkelen van de OV-chipkaart, geopperd door diverse betrokkenen. Ik vat ze hieronder samen.

I. "*Stoppen*"
   Er wordt geen OV-chipkaart ingevoerd dan wel verder uitgerold.
II. "*Enkelvoudige kaartinfrastructuur Mifare Classic*"
   De huidige OV-chipkaart, gebaseerd op de Mifare Classic, wordt verder uitgerold.
III. "*Dubbele kaartinfrastructuur Mifare Classic + opvolger*"
   De huidige OV-chipkaart, gebaseerd op de Mifare Classic, wordt verder uitgerold, en op termijn worden de kaarten vervangen door kaarten met een chip die beter beveiligd is dan de Mifare Classic. Aan de rest van de infrastructuur, i.h.b. de backoffice, wordt niet getornd.
IV. "*Enkelvoudige kaartinfrastructuur opvolger*"
   De huidige OV-chipkaart, gebaseerd op de Mifare Classic, wordt *niet* verder uitgerold. De kaarten worden zo snel mogelijk vervangen door kaarten met een chip die beter beveiligd is dan de Mifare Classic. Aan de rest van de infrastructuur, i.h.b. de backoffice, wordt niet getornd.
V. "*OV-chip 2.0*"
   De huidige OV-chipkaart wordt niet verder uitgerold. Er wordt, in een nieuwe digitale infrastructuur ontworpen voor zowel de kaart als de backoffice. Het ontworpen systeem zal dezelfde functionaliteit kennen als de huidige OV-chipkaart, of zelfs betere, maar dan goed beveiligd zijn en ook harde privacygaranties bieden aan de reiziger. Bovendien zal het een *open systeem* zijn, in die zin dat iedere wetenschapper en hacker kan verifiëren dat het systeem inderdaad deze eigenschappen bezit.

Ik zal kort op deze scenario's ingaan.

II. Het verder uitrollen van een kaart die stuk is, lijkt mij onverstandig. De OV-chipkaart is drager van geld (d.w.z. reistegoed), en als die drager relatief eenvoudig te manipuleren is, kan

dit tot financiële schade leiden. Maatregelen die de financiële risico's beperken, zoals het blokkeren van gekloonde kaarten, zullen ook eerlijke reizigers grote ongemakken opleveren.

III. Het voeren van een dubbele kaartinfrastructuur neemt alle risico's van de Mifare Classic met zich mee. Bovendien is een dergelijke infrastructuur bijzonder complex en vatbaar voor allerhande problemen. Gezien het feit dat de enkelvoudige kaartinfrastructuur met de Mifare Classic verschillende kinderziekten heeft, zijn de nodige reserves bij dergelijke "oplossing" gerechtvaardigd.
IV. De problemen van de Mifare Classic die o.a. door de Radboud Universiteit Nijmegen zijn aangekaart, worden opgelost door het overstappen op een betere chip. Echter, de backoffice van het systeem is dan nog steeds geheim, en zou wellicht andere problemen kunnen bergen. Ook is dan het privacyprobleem nog niet opgelost.
V. Soms is het verstandig als een computersysteem te veel problemen geeft, maar gewoon overnieuw te beginnen. Dat biedt de mogelijkheid enkele andere liggende problemen ook gelijk op te lossen, zoals bijvoorbeeld de geslotenheid van het systeem en de welhaast Orwelliaanse privacy-eigenschappen van het huidige systeem. Als wetenschapper heeft deze optie mijn uitdrukkelijke voorkeur. Het publieke vertrouwen in de kaart kan ook gebaat zijn bij een oplossing waarvan wetenschappers en hackers hebben kunnen controleren dat deze geen hiaten geeft.

Bij de scenario's III, IV en V zijn aanpassingen aan de (reeds geplaatste) poortjes nodig: behalve de kaart zal hoogstwaarschijnlijk ook de "kaartlezer" vervangen moeten worden.

Tot slot

Tot slot van deze brief hecht ik er aan alvast enkele zaken in hun context te plaatsen.

In het recente verleden is door enkele betrokken partijen benadrukt dat de OV-chipkaart, zelfs met de gebroken Mifare Classic, de privacy voldoende beschermt. Het is inderdaad zo, dat iemand die een vreemde OV-chipkaart in handen krijgt, niet in staat is de rechtmatige eigenaar "uit te kleden" en al diens gedragingen bloot te leggen. De vervoersbedrijven kunnen dit echter wel. Individueel reisgedrag kan gevolgd en gebruikt worden voor onder andere marketing en datamining. Voor het goede functioneren van het systeem is dit echter absoluut niet nodig.

Het "wetenschapsforum OV-chipkaart" is een geschikte plaats om de "OV-chip 2.0" verder uit te werken. TLS heeft haar (inhoudelijke) medewerking aan dit forum toegezegd.

In alle gepubliceerde plannen over het beteugelen van de problemen met de OV-chipkaart heb ik de problemen met de dagkaart niet meer terug gevonden. Het probleem met de dagkaart, waarin de Mifare Ultralight chip zit, is dat deze *helemaal geen beveiliging kent*. In januari demonstreerde Radboud-student Roel Verdult dat je daardoor met een eenvoudig apparaat, de "Ghost", onbeperkt gratis in het openbaar vervoer kunt reizen, en tóch bij kaartcontrole een geldig plaatsbewijs kunt tonen. Een plan dat dit feit negeert bekijk ik met zorg.

Ik kijk uit naar de hoorzitting op 18 juni, waar ik bovenstaande (en andere) punten desgevraagd graag nader met u bespreek. Voor de goede orde meld ik dat ik deze brief als openbaar beschouw.

Hoogachtend,

dr. W.G. (Wouter) Teepe