Ov-chipkaart definitief gehackt

Maandag 10 maart 2008, 00:01 - Een nieuw onderzoek toont aan dat dieven reistegoeden van de ov-chipkaarten van medepassagiers kunnen stelen. TNO wuifde het risico van zo'n aanval eerder juist weg.

Door **Brenno de Winter**

De Duitse onderzoekers Karsten Nohl en Henryk Plötz hebben een **paper** (pdf) gepubliceerd waarin een manier beschrijven waarmee zij de sleutel van de Mifare Classic chip kunnen achterhalen. Met die sleutel kunnen programmeurs de informatie op de chip lezen, kopiëren en wijzigen.

De chip wordt onder meer toegepast in de OV-chipkaart. Vorig jaar december brachten Nohl en Plötz al de **zwakke plekken in kaart**, maar kraakten de versleuteling nog niet. Dat is nu wel gelukt, zo blijkt uit het rapport.

Volgens Nohl is het nu mogelijk om **kopieën te maken** van de chips van bijvoorbeeld medereizigers, en daarmee het tegoed van die kaarten te stelen, zo vertelt de hacker tegen Webwereld. Het is waarschijnlijk niet mogelijk om zelf het tegoed op te waarderen, omdat de vervoersbedrijven dat eenvoudig zelf centraal kunnen controleren.

Dieven zouden zich kunnen richten op reizigers die zojuist hun chipkaart hebben opgeladen, om die vervolgens te kopiëren. De crimineel zou dan zelf gratis kunnen reizen. "Op het moment dat het tegoed verbruikt is, geeft dat niet want dan steel je gewoon van de volgende kaart," zegt Nohl.

TNO-rapport

Een **rapport** (pdf) dat TNO in opdracht van Trans Link Systems **opstelde**, suste vorige maand juist nog de ophef rond de chip. De TNO-onderzoekers schreven dat de kans op fraude beperkt is, omdat aanvallers zware middelen moesten inzetten om daadwerkelijk misbruik van de kaart te maken. Dat zou voor dieven teveel werk zijn.

Trans Link is verantwoordelijk voor de invoering van de ov-chipkaart en greep het rapport aan om onveranderd door te gaan met de invoering van de chipkaart.

De bevindingen van Nohl en Plötz staan lijnrecht tegenover het TNO-rapport. Nohl waarschuwt dat de gaten in de Mifare chip breed misbruikt kunnen worden. De rfid-chip wordt namelijk niet alleen ingezet voor de ov-chipkaart maar voor andere toepassingen. Zo loopt in het noorden van het Verenigd Koninkrijk proef met elektronisch betalen in winkels die gebaseerd is op de Mifare. Bij dergelijke projecten zou misbruik eenvoudiger en lucratiever zijn.

Scepsis

Na bestudering van het document van Nohl en Plötz meent ook Bart Jacobs, hoogleraar informatiebeveiliging aan de Radboud Universiteit in Nijmegen, dat het TNO-onderzoek grote fouten bevat. Hij is vooral kritisch over de constatering dat de kaart alleen met dure apparatuur te kraken zou zijn. Toch wacht hij met een definitieve conclusie tot de onderzoekers met harde bewijzen komen: "Ik kan me niet aan de indruk onttrekken dat hier te vroeg geclaimd wordt", zegt hij in een reactie. "Maar ondertussen denk ik dat het niet lang meer duurt voordat de kaart omvalt."

Jacobs heeft eerder meegewerkt aan onderzoek waarbij studenten een **dagkaart wisten te klonen** waardoor zij gratis konden reizen. De dagkaart is minder zwaar beveiligd dan de kaart voor abonnementen.

Voor hacker en activist Rop Gonggrijp is de paper wel overtuigend. Met de kennis over de structuur van de chip is het nu eenvoudig om de sleutel te achterhalen. "Daar hoef je niet eens een paper voor te schrijven, dat weet elke cryptograaf ook zo", zegt hij. Hij ziet dan ook geen toekomst voor de OV-Chipkaart: "Tenzij Karsten en Henryk helemaal liegen (en waarom zouden ze?), is Mifare Classic stuk. Helemaal onbruikbaar stuk."

Proof of Concept

Nohl wil zijn hack voorlopig nog niet demonstreren. "We willen eerst de de discussie starten, zodat mensen tijd hebben het systeem aan te passen of te stoppen. Dus reken nog niet op een demonstratie in het veld, maar daar komen we wel voor de zomer mee", zegt hij. "De *proof of concept* zouden we nu al kunnen doen, maar we willen eerst de mensen de tijd geven te handelen."

Gonggrijp benadrukt echter dat een vastberaden aanvaller de chip nu al moet kunnen hacken. "Zelfs met de informatie die nu publiek is is het in principe te doen, maar het is meer werk en niemand gaat daar eens echt goed voor zitten omdat men weet dat over een paar maanden toch vanzelf uit de lucht komt vallen."

Tags: **tno**, **beveiliging**, **aanval**, **hack**, **translink**, **mifare**, **chipkaart**, **ov-chipkaart**.

Security: **Bekijk meer security nieuws, blogs, downloads en presentaties.**

pdf bijlagen

ovchip (146,05 Kb)