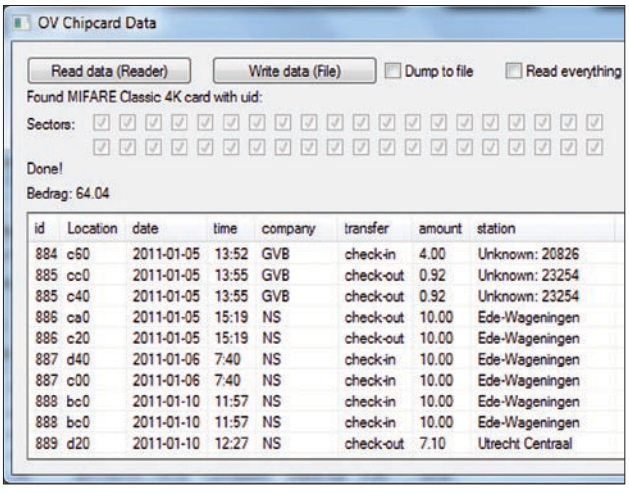
BEVEILIGING CHIPKAART WERKT NIET

# GRATIS REIZEN KAN

TEKST: **BRENNO DE WINTER**

Dat de Linux-tools het lezen van een OV-chipkaart goed mogelijk maken, weten we inmiddels. Maar dankzij een Windows-tool, waarmee u de kaart óók kunt beschrijven, is het voor iedereen een fluitje van een cent om de kaart te hacken en gratis te reizen. De controleur ziet niets verdachts en de kaart blijft – tegen de belofte in – gewoon actief.

De eerste hacks van de OV-chipkaart werden door de verantwoordelijken weggewuifd met het argument dat het zo'n vaart niet zou lopen omdat de meeste mensen toch met Windows werken. Daarom zou niet iedereen met de software aan de slag kunnen. In PC-Active 243 schreven we al dat het een kwestie van tijd was voordat de Windows-tools beschikbaar zouden zijn. Inmiddels is dat moment aangebroken en kan iedereen met een beetje computerkennis aan de slag om zijn OV-chipkaart uit te lezen. Maar we gaan verder en we nemen de proef op de som en we bekijken of 'lezen' ook 'schrijven' betekent. Met andere woorden: kunnen we 'onbeperkt' blijven reizen op een eenmaal aangeschaft saldo? Of wordt de kaart geblokkeerd omdat fraude wordt gedetecteerd, zoals Trans Links Systems ons keer op keer belooft? De uitkomsten van ons onderzoek zijn zeer verrassend!




| id | Location | date | time | company | transfer | amount | station |
|---|---|---|---|---|---|---|---|
| 884 | c60 | 2011-01-05 | 13:52 | GVB | check-in | 4.00 | Unknown: 20826 |
| 885 | cc0 | 2011-01-05 | 13:55 | GVB | check-out | 0.92 | Unknown: 23254 |
| 885 | c40 | 2011-01-05 | 13:55 | GVB | check-out | 0.92 | Unknown: 23254 |
| 886 | ca0 | 2011-01-05 | 15:19 | NS | check-out | 10.00 | Ede-Wageningen |
| 886 | c20 | 2011-01-05 | 15:19 | NS | check-out | 10.00 | Ede-Wageningen |
| 887 | d40 | 2011-01-06 | 7:40 | NS | check-in | 10.00 | Ede-Wageningen |
| 887 | c00 | 2011-01-06 | 7:40 | NS | check-in | 10.00 | Ede-Wageningen |
| 888 | bc0 | 2011-01-10 | 11:57 | NS | check-in | 10.00 | Ede-Wageningen |
| 888 | bc0 | 2011-01-10 | 11:57 | NS | check-in | 10.00 | Ede-Wageningen |
| 889 | d20 | 2011-01-10 | 12:27 | NS | check-out | 7.10 | Utrecht Centraal |

*De gegevens van een willekeurige OV-chipkaart*

## Gratis reizen binnen handbereik

Kunt u met de nieuwe software nu zwartrijden? Het antwoord is overduidelijk: ja. Als we met de nieuwe software onze kaart uitlezen (zie ook verderop in het artikel) valt ons op dat tussen de transacties ook een transactienummer zit. Dit nummer loopt op en is – zo vermoeden wij – ook nog ergens op de kaart opgeslagen. Wie daarmee gaat rommelen, loopt waarschijnlijk tegen de lamp en dat is natuurlijk niet de bedoeling. Het is dus handiger om geld op de kaart te storten, een dump (exacte kopie) van de gegevens te maken en die dump na het reizen terug te zetten. We kopen daarom een anonieme OV-chipkaart bij een NS-automaat en we zetten er € 5 op. Daarna maken we direct een dump van de kaart.

We nemen de bus en checken netjes in- en uit. Na het reizen zetten we de reservekopie terug op de kaart en, voilá we hebben weer een OV-chipkaart in onze handen met € 5 tegoed en geen enkele geregistreerde transactie! We nemen opnieuw de bus en stappen ook nog een keertje over. Vervolgens maken we een ritje met de metro en als die rit achter de rug is, zetten we de back-up weer terug. Opnieuw hebben we een kaart waar op het eerste gezicht nog nooit mee is gereisd… Een spannend moment is dan ook als een controleur de bus instapt. We tonen onze gekraakte kaart, hij controleert en … ontdekt niets. Natuurlijk is dit veel gedoe voor weinig, maar het mag duidelijk zijn dat als dit met € 5 kan, het ook mogelijk is met € 100.

Het volledige artikel is te lezen in het februarinummer van PC-Active, dat vanaf vrijdag 28 januari 2011 in de winkel ligt.