UvA UNIVERSITEIT VAN AMSTERDAM

Het leven wordt steeds gemakkelijker.

Security evaluation of the disposable OV-chipkaart

Maurits van der Schee
Pieter Siekerman

July 4, 2007

Master System and Network Engineering
University of Amsterdam

Nederland telt steeds meer alleenstaanden

DEN HAAG — Het aantal alleenstaanden in Nederland blijft toenemen. Ruim 20 procent van de Nederlandse bevolking woont in 2050 alleen. Dat percentage lag in 2006 nog op 15. Dat bleek gisteren uit cijfers van het Centraal Bureau van de Statistiek (CBS).

Net als in 2006 voert ook in 2050 een meerderheid van de Nederlanders een huishouden met kinderen. Dat aantal neemt de komende decennia wel af. Na 2034 krimpt de bevolking van Nederland. Verwacht wordt dat er in 2060 ruim 90.000 gezinnen met jonge kinderen minder zijn dan in 2006. Toen waren er 900.000 gezinnen met een jongste kind jonger dan zes jaar. (ANP)

Hbo-docent moet kennis vergroten

DEN HAAG — Hogescholen hebben tot 2010 een bedrag dat oploopt tot € 215 miljoen nodig om het vak van docent verder te professionaliseren. Minister Plasterk (Onderwijs) zou € 100 miljoen moeten bijdragen, het overige deel komt voor rekening van de hogescholen.

Dat schreven de HBO-raad en enkele vakbonden gisteren in het manifest 'Toekomstperspectief voor hogeschool en medewerker'. Dit jaar is volgens het manifest een extra investering van € 25 miljoen noodzakelijk. Het geld is, behalve voor hogere salarissen, ook bedoeld om docenten te stimuleren lan-

Fouten in software van kaartlezers chipkaarten

door John Maes

AMSTERDAM — Twee studenten van de masteropleiding System and Network Engineering aan de Universiteit van Amsterdam (UvA) hebben tijdens hun afstudeeronderzoek een lacune gevonden in de beveiliging van de papieren variant van de ov-chipkaart. Dat is de versie die vooral door toeristen wordt gebruikt. Door de fout is in principe vrij reizen mogelijk.

De fout is gevonden bij de poortjes van het GVB (Amsterdam), maar waarschijnlijk is de lacune er ook bij de RET (Rotterdam). Maurits van der Schee (27) en Pieter Siekerman (24) studeren morgen af op hun onderzoek, dat vier weken heeft geduurd. Al in de tweede week van hun (zelfgekozen) onderzoek brachten ze met een zogenoemde RFID-kaartlezer ter waarde van € 148 de lacune aan het licht. Door de fout kon de wegwerpkaart, na herprogrammering, opnieuw worden gebruikt.

De studenten zeggen de lacune louter met goede bedoelingen te hebben aangetoond. De details houden de studenten nog achter totdat het gat in de beveiliging is opgelost, zegt Maurits van der Schee. „Iedereen met zo'n kaartlezer kan de chipkaart tot die tijd ook manipuleren."

Van der Schee en Siekerman hebben inmiddels een baan aangeboden gekregen bij Trans Link, het bedrijf dat de ov-chipkaart maakt in opdracht van Connexxion, GVB, HTM (Den Haag), NS en RET. Dr. ir. Cees de Laat, begeleider van de studenten, heeft gemengde gevoelens bij hun vertrek. „Studenten die afstuderen aan de opleiding System and Network Engineering hebben bij hun afstuderen al meerdere aanbiedingen op zak. Maar zo wordt het wel moeilijk om ze vast te houden voor de wetenschap."

Trans Link Systems, speciaal opgericht om het nationale ov-chipkaartsysteem voor het openbaar vervoer te realiseren, laat in een persbericht weten tevreden te zijn met het onderzoek. Jannemieke Zandee van Trans Link: „De studenten hebben een constructieve en waardevolle bijdrage geleverd aan de ontwikkeling en beveili-

Dierenasiels stromen vol

Een medewerker van een dierenasiel in Rotterdam haalt een groepje kittens aan. Veel dierenasiels zitten al voor het begin van de zomervakantie vol. De Dierenbescherming bevestigt dat beeld en zegt dat asiels snel een opnamestop moeten invoeren. „We zien al jaren dat asielen snel vol raken. Nederland heeft te maken met een immer groeiend kattenprobleem", aldus een woordvoerder. FOTO: ANP

Minder agressief r voedingssupplem

DEN HAAG — Gevangen extra voedingssupplement bruiken, vertonen minder a sief gedrag. Dat is gebleke een onderzoek van de D Justitiële Inrichtingen (DJ

De studie biedt nog c doende houvast voor con maatregelen om agressie b detineerden via voeding teugelen. Daarvoor moet nader worden gekeken na effecten van voedingssu menten, het liefst onder pl van gewelddadige delicter maakte de DJI gisteren bek

De dienst keek sinds 2005 samen met de Rad Universiteit Nijmegen in verre extra voeding kan h bij het terugdringen van s sief gedrag. Aan het onde deden 221 jongvolwassen tineerden mee van 18 t jaar. (

'Liever minder d meer werken'

AMSTERDAM — Terwij tekort aan personeel toen en vacatures moeilijker ve baar worden, zijn maar w werknemers bereid om me gaan werken om zo toch werk gedaan te krijgen meeste werkenden willen minder uren per week dra Dat blijkt uit verschillen ternetpeilingen onder 2 tot 31.000 bezoekers www.postbank.nl, die gis zijn gepubliceerd. Van de b kersstelt twee derde er ge hoefte aan te hebben me

INTERNET

Gratis reizen door fout in ov-chipsysteem

Uitgegeven: 2 juli 2007 14:32
Laatst gewijzigd: 2 juli 2007 14:35

AMSTERDAM - Een fout in de software van de toegangspoortjes maakt het mogelijk met chipkaarten zwart te reizen in tram, bus en metro in Amsterdam en Rotterdam. Dat ontdekten studenten van de Universiteit van Amsterdam (UvA).

Het gaat om een fout in de software die de geldigheid controleert van wegwerpkaartjes. Die kaartjes, die voornamelijk worden verkocht aan toeristen, zijn beperkt geldig en minder streng beveiligd dan de persoonsgebonden chipkaarten. Door de

Podcast

Best gelezen

1. Software iPhone lekt uit op internet

Contents

- Why?
- What is the OV-chipkaart?
- How did we do our research?
- Card data
- Transactions
- Vulnerabilities
- Recommendations
- Epilogue

Why?

- Interesting subject
- Vital infrastructure
- No technical information publicly available
- To improve the system, NOT to promote abuse

OV-chipkaart

- National public transport payment card
- RFID-based contactless technology
- Trans Link Systems
- Amsterdam & Rotterdam
- Launch: January 1, 2009

THALES

Types of cards

- Disposable paper card

How?

- Public documentation of Mifare Ultralight
- Observation of data
- Manipulation of data
- Lots and lots of trial and error

Contents of a disposable card

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- 512 bits: 16 pages of 4 bytes each

Unique Identifier

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- Set during manufacture, cannot be changed

Lock Bytes

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- Restrict access to parts of memory to read-only

One Time Programmable (OTP) Counter

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- 1111 1111 1111 1000
- Irreversible counter used to track remaining

User Area

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- Fully read-write accessible

Card Details

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- General characteristics: type of card, expiration date

Transactions

```
04989B8F D1D20280 814800F0 DF33FFF8
C8002002 277CA7C0 0687CB77 8F9D119E
C8001002 077CA7C0 9B355ECC 3988DAB6
8E416418 8BB36A4C 1B2F858F 8062A79B
```

- Last 2 transactions are saved
- Oldest transaction replaced by new transaction

Transactions

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Transaction counter

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

City?

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Transaction type

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Date

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Time

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Encrypted (Station and integrity)

```
C8001002 07732D30 0A920530 5B6EFF53
C8002002 27732E60 26804B14 413F9D8B
C0003002 47733000 CCD18C5C 656C88AE
C8004002 27733100 018EC4DD 13051785
C0005002 47733130 EA535D22 D2D497EC
C0006002 C7733160 BC96C921 18E8911E
B8007002 47733190 C2D75857 051705D3
C8008002 27733240 266BA19B B133BA2A
```

Example

C8001002 07732D30 0A920530 5B6EFF53

- 001 = Transaction 1
- 002 = Amsterdam
- 0 = Purchase
- 773 = June 12, 2007
- 2D3 = 12:03

Vulnerabilities

- Disabled defence mechanism
  - Allows repeated attacks with one card
- Repeated check-out
  - Ride counter is only increased during check-in
- Free travel
  - We could tell you, but then we would have to kill you

Recommendations

- Open approach to security research: make detailed technical information about the OV-chipkaart public
- Encrypt all data on the Mifare Ultralight cards …
- … or stop using Mifare Ultralight cards
- Improve public information and employee knowledge

Epilogue

- Constructive contact with Trans Link Systems
- Combined press release
- Vulnerability remains confidential until the problem has been solved
- The dilemma of ethical hacking

UvA UNIVERSITEIT VAN AMSTERDAM

Het leven wordt steeds gemakkelijker.

Questions?