SECURITY OF LOYALTY CARDS USED IN ESTONIA

Name: Danielle Morgan
Supervisor: Rain Ottis
Co-Supervisor: Arnis Paršovs
LOYALTY CARDS

Loyalty schemes are offered by merchants to provide repeat customers with benefits and discounts. Loyalty cards are used to identify these customers.

Objective: Study card resistance to cloning attacks

Types:
- Magnetic-Stripe
- Contactless
- ID Card
MAGNETIC-STRIPE CARDS

• Have 3 tracks — only one mainly used
  • Track 2 which generally stores card number
  • 9233707233773183=19050000000000000000

• Magnetic-stripe cards allow cloning by default

• The goal however is to gain the track information without having to physically swipe the card
# Magnetic-Stripe Cards

## List of Cards
1. ABC Card
2. Aitäh Card
3. Club One Card
4. Hesburger Card
5. ISIC Card
6. Koduekstra Card
7. Partner Card
8. Säästu Card
9. PINS Card
10. Rimi Card

## Track 1
### User Data
B2106574003381003^DANIELLE/MORGAN
^9912799991210000400338100300000

## Track 2
- Card Number
- Expiration Date
- Service Code
- Additional Data

## Track 3
Security Information
9002=1233000107609866=000000000=944038520
0=01=000000=00=201231=160519=0233
SUMMARY FOR MAGNETIC-STRIPE CARDS

• Cards can be cloned without reading magstripe:
  • Information can be found on the card surface
  • Information also on the receipts
• Difficult to clone design of the card
  • Self-service terminals remove the need
CONTACTLESS CARDS

Low Frequency Cards (125kHz)
• MyFitness Card
  • Write protected
  • Easily cloned

MIFARE DESFIRE EV1
• Elron Card
  • Possibly several files stored in Elron application
  • Read/Write access requires authentication key
  • Card could not be cloned – reading keys unknown
CONTACTLESS CARDS

MIFARE Classic 1K
- Tallinn Bus Card
  - Can be publicly read
  - Keys for writing can be recovered
  - Can be cloned using UID-changeable cards or

- ISIC / SEB ISIC
  - Partially readable
  - Write keys not recoverable
  - Clone made using UID changeable card or Chameleon
SERVICES USING MIFARE CLASSIC CARDS

- Pilveprint
  - Can be cloned using a standard MIFARE Classic card

Smart Bike Lock
Easily cloned with UID changeable card as it relies only on UID

TTU Gym
Cloned using UID-changeable card – also only uses UID
CONTACTLESS CARDS

MIFARE Ultralight C
• Tartu Bus Card
  • Fully readable and writable
  • Default write key “BREAKMEIFYOUCAN!”
  • Cloneable with a UID changeable card

• Rimi Card
  • Partially readable and writable
  • Keys unknown
  • Not cloneable without full read access
CONTACTLESS CARDS SUMMARY

• Most cards cloneable

• Rimi and Elron cards not cloneable
  • Used symmetric keys to prevent reading
  • If key found all cards may be cloned
ESTONIAN ID CARD AS A LOYALTY CARD

<table>
<thead>
<tr>
<th>Record</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Surname</td>
</tr>
<tr>
<td>2</td>
<td>First name line 1</td>
</tr>
<tr>
<td>3</td>
<td>First name line 2</td>
</tr>
<tr>
<td>4</td>
<td>Gender: “M” – Male, “N” – Female</td>
</tr>
<tr>
<td>5</td>
<td>Nationality</td>
</tr>
<tr>
<td>6</td>
<td>Birth date (dd.mm.yyyy)</td>
</tr>
<tr>
<td>7</td>
<td>Personal ID code</td>
</tr>
<tr>
<td>8</td>
<td>Document Number</td>
</tr>
<tr>
<td>9</td>
<td>Document Expiry Date</td>
</tr>
<tr>
<td>10</td>
<td>Place of Birth</td>
</tr>
<tr>
<td>11</td>
<td>Date of Issuance</td>
</tr>
<tr>
<td>12</td>
<td>Type of Residence Permit</td>
</tr>
<tr>
<td>13 - 16</td>
<td>Notes Line 1 - 4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APDU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 a4 02 0c 02 50 44</td>
<td>Select Personal Data File</td>
</tr>
<tr>
<td>00 b2 01 04 00</td>
<td>Read Surname</td>
</tr>
<tr>
<td>00 b2 02 04 00</td>
<td>Read First name line 1</td>
</tr>
<tr>
<td>00 b2 03 04 00</td>
<td>Read First name line 2</td>
</tr>
<tr>
<td>00 b2 04 04 00</td>
<td>Read Gender</td>
</tr>
<tr>
<td>00 b2 05 04 00</td>
<td>Read Nationality</td>
</tr>
<tr>
<td>00 b2 06 04 00</td>
<td>Read Birth date</td>
</tr>
<tr>
<td>00 b2 07 04 00</td>
<td>Read Personal ID code</td>
</tr>
<tr>
<td>00 b2 08 04 00</td>
<td>Read Document number</td>
</tr>
</tbody>
</table>
FAKE ID CARD

1) Java Card – programmable smart card

2) Based on FakeEstEID applet by Martin Paljak
   https://github.com/martinpaljak/esteid-applets/blob/master/docs/FakeEstEID.md

Applet modified to log commands received

Arbitrary personal data file contents can be set

RSA keys cannot be copied
## Results

### Merchants where card was tested
- Forum Cinemas
- Olerex
- Pilveprint
- Prisma
- TTU Library

<table>
<thead>
<tr>
<th>APDU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 a4 01 0c 02 ee ee</td>
<td>Select EstEID Dedicated File</td>
</tr>
<tr>
<td>00 a4 02 04 02 50 44</td>
<td>Select Personal Data File</td>
</tr>
<tr>
<td>00 b2 08 04 00</td>
<td>Read Document number</td>
</tr>
<tr>
<td>00 b2 09 04 00</td>
<td>Read Expiry date</td>
</tr>
</tbody>
</table>

#### Prisma

<table>
<thead>
<tr>
<th>APDU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 a4 01 0c 02 ee ee</td>
<td>Select EstEID Dedicated File</td>
</tr>
<tr>
<td>00 a4 02 04 02 50 44</td>
<td>Select Personal Data File</td>
</tr>
<tr>
<td>00 b2 07 04 00</td>
<td>Read Personal ID code</td>
</tr>
<tr>
<td>00 b2 08 04 00</td>
<td>Read Document number</td>
</tr>
<tr>
<td>00 b2 09 04 00</td>
<td>Read Expiry date</td>
</tr>
</tbody>
</table>
SUMMARY

• Most of the loyalty cards can be cloned
• Large scale fraud not expected
  • Small amounts
  • Hard to monetize
  • Trace left
RECOMMENDATIONS

• NFC protective cover
• Cardholder identity verification for large transactions
• ID card could serve as universal uncloneable loyalty card
  • Has to be enabled
  • Has to be used by merchants
THE END

Questions

Comments

Queries