

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

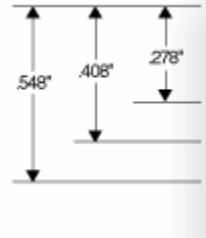


Diagram showing the dimensions of a magnetic stripe: total width .548", Track 1 width .408", and Track 2 width .278".

	0.223"		Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

- 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

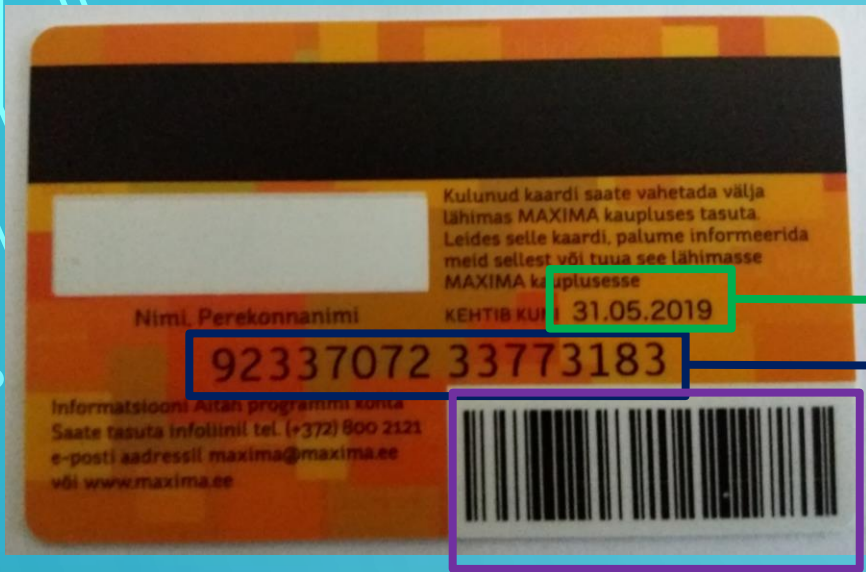
Track 2

- Card Number
- Expiration Date
- Service Code
- Additional Data

Track 3

Security Information

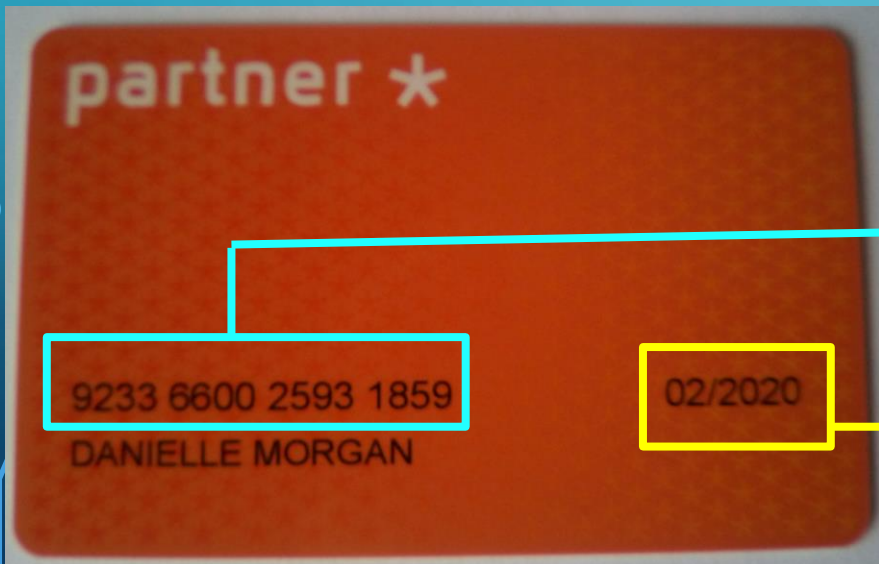
9002=1233000107609866=000000000=944038520
0=01=000000=000=201231=160519=0233



Track 2

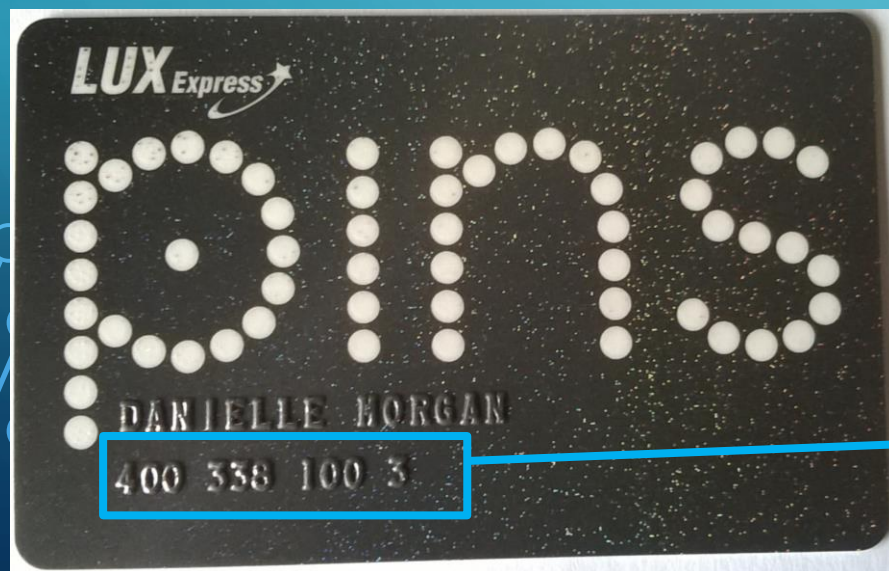
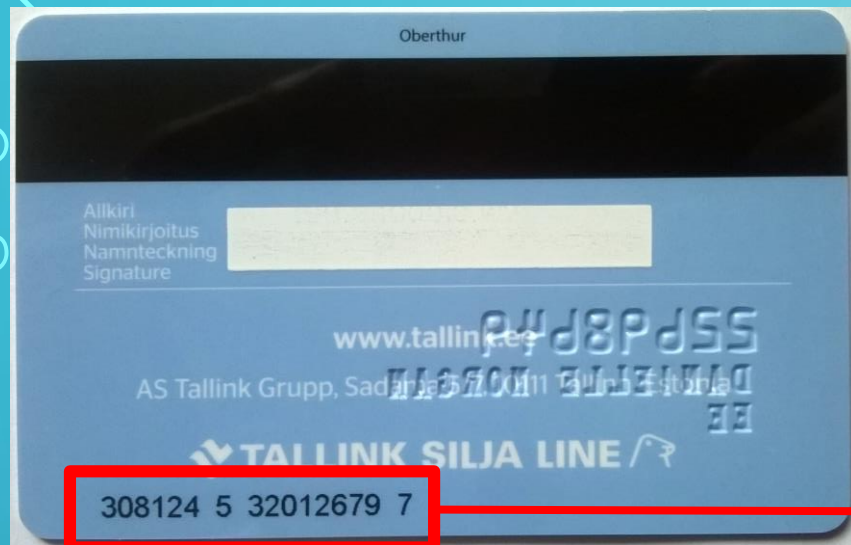
9233707233773183=19050000000000000000

D23377318319057



Track 2

9233660025931859=20025010000000000000



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

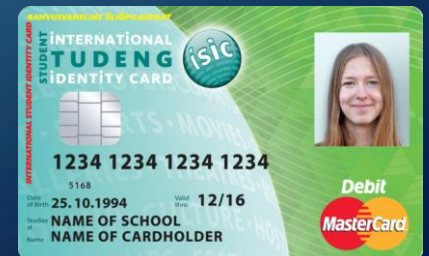


MIFARE Classic 1K

- 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



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

APDU	Description
00 a4 02 0c 02 50 44	Select Personal Data File
00 b2 01 04 00	Read Surname
00 b2 02 04 00	Read First name line 1
00 b2 03 04 00	Read First name line 2
00 b2 04 04 00	Read Gender
00 b2 05 04 00	Read Nationality
00 b2 06 04 00	Read Birth date
00 b2 07 04 00	Read Personal ID code
00 b2 08 04 00	Read Document number

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

Pilveprint

APDU	Description
00 a4 01 04 02 ee ee	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 08 04 00	Read Document number

APDU	Description
00 a4 01 0c 02 ee ee	Select EstEID Dedicated File
00 a4 02 04 02 50 44	Select Personal Data File
00 b2 07 04 00	Read Personal ID code
00 b2 08 04 00	Read Document number
00 b2 09 04 00	Read Expiry date

Prisma

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 slide features a blue gradient background with decorative white circuit-like lines in the corners. These lines consist of straight segments and small circles, resembling a stylized electronic circuit or data paths.

THE END

Questions

Comments

Queries