NFC Payment Spy: A Privacy Attack on Contactless Payments

Maryam Mehrnezhad, Mohammed Ali, Feng Hao, Aad van Moorsel

Newcastle University, UK

SSR, 5 Dec 2016

Contactless Payment

- Contactless Cards (theukcardsassociation.org.uk)
  - In the UK in Feb 2016
  - £1,318.3 m contactless card payment
  - An increase of 306.8% per the year
- Other NFC payment technologies
  - Mobile phones, tablets, watches, bPay bands/stickers, Visa-powered payment ring (Rio 2016 Olympics)
  - Over 350 different brands/models of NFC-enabled devices in the market (nfcworld.com)

What happens if there are multiple contactless cards in the reader's field?

Card Clash: Oystercard and contactless bank cards

- Well-publicised phenomenon (the Guardian and TfL)
- While swiping a wallet on a reader paying for travel with a card did not intend
- More expensive, double charged
  - Weekly travelcard
  - Touch in and out with different cards
- Applying for a refund by checking online accounts
  - Provided by Transport for London
  - TfL handed back £300,000 to 50,000 customers within 3-5 working days (2014)

Suggested Solutions

- Taking the card off from the wallet
- Checking online accounts and claim the refund
- Use protective cases for cards
- Switch to contactless payment (no Oystercard)
- Using other technologies (bPay band, mobile)

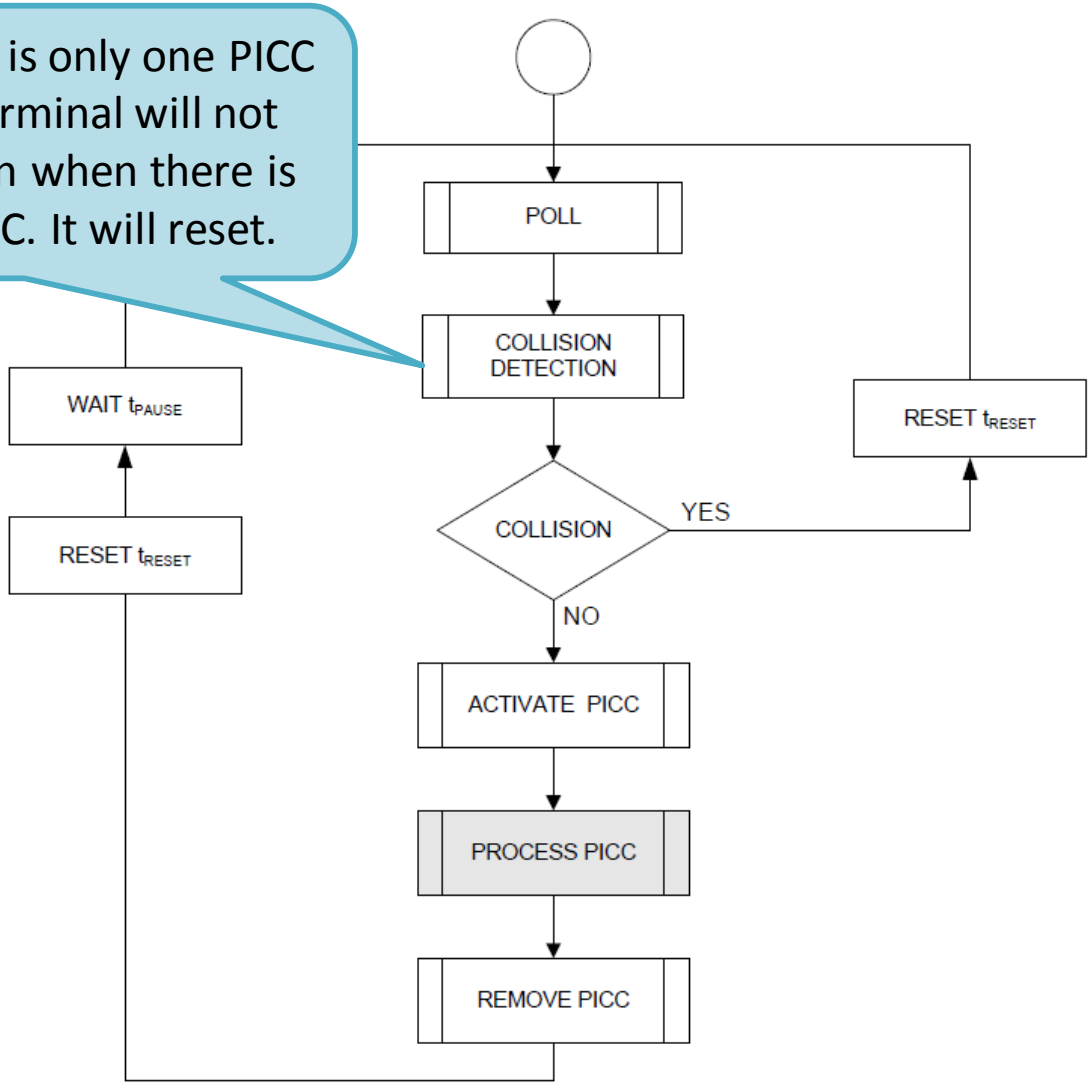
What do Standards Specify?

- EMV: the primary standard for contactless card payments
- ISO/IEC 1443: the main standard for proximity cards including payment

EMV Contactless Book D- Card Collision

Figure 9.1: Terminal Main Loop

To ensure that there is only one PICC in the Field. The terminal will not initiate a transaction when there is more than one PICC. It will reset.



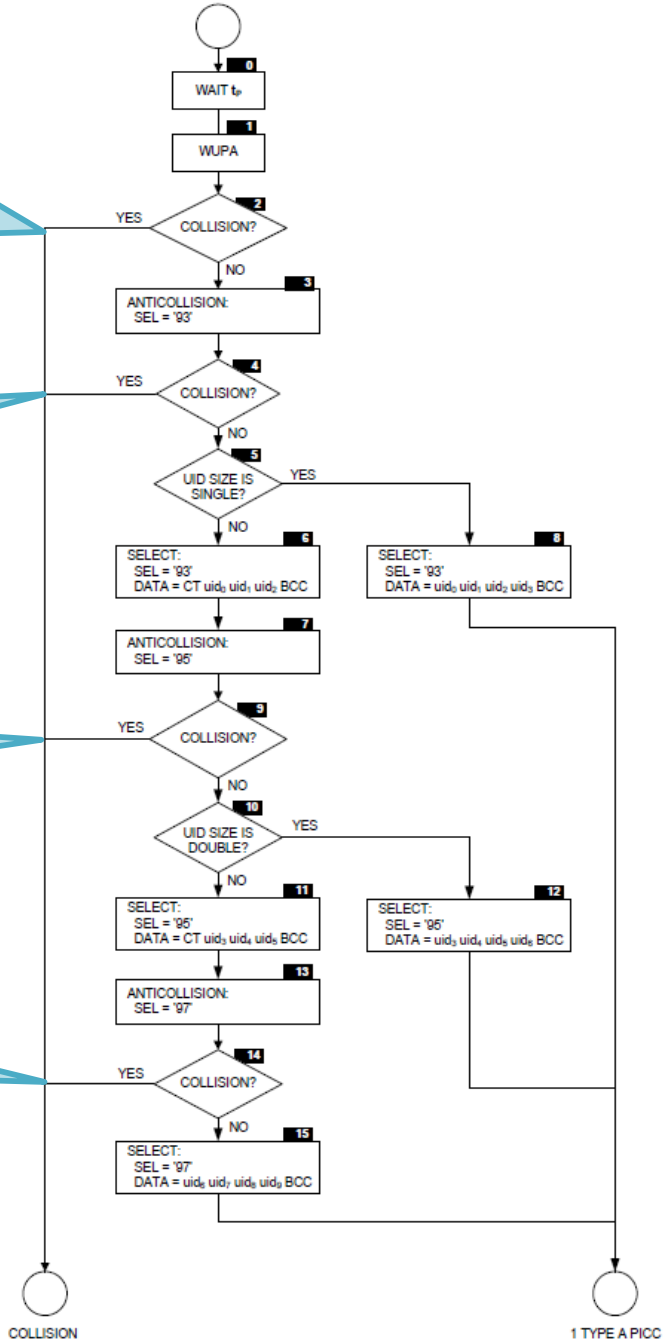
If more than a technology is in the field or collision is detected during the WUPA command

Collision detected at first 4 bytes of UIDs

Collision detected at first 7 bytes of UIDs

Collision detected at first 10 bytes of UIDs

Figure 9.3: Type A Collision Detection



EMV Spec- Card Collision

- Regardless of the collision procedure, once a collision is detected, the terminal should not proceed any more; instead it should reset the field and go back to the polling procedure

ISO/IEC 1443-3 standards

6.5.1 Select sequence flowchart

The select sequence is specified in Figure 9.

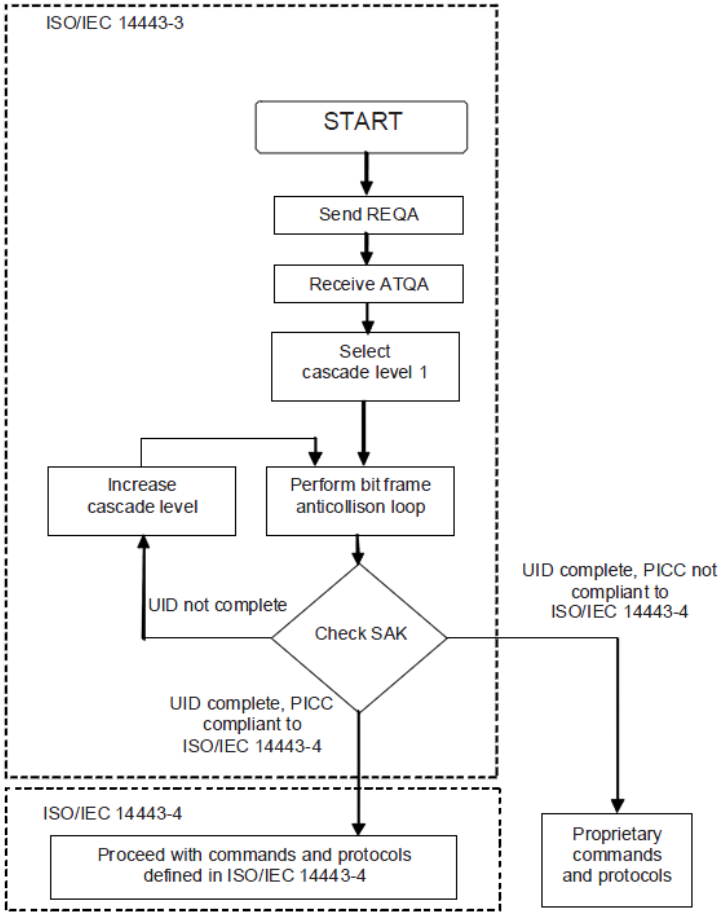


Figure 9 — Initialization and anticollision flowchart for PCD

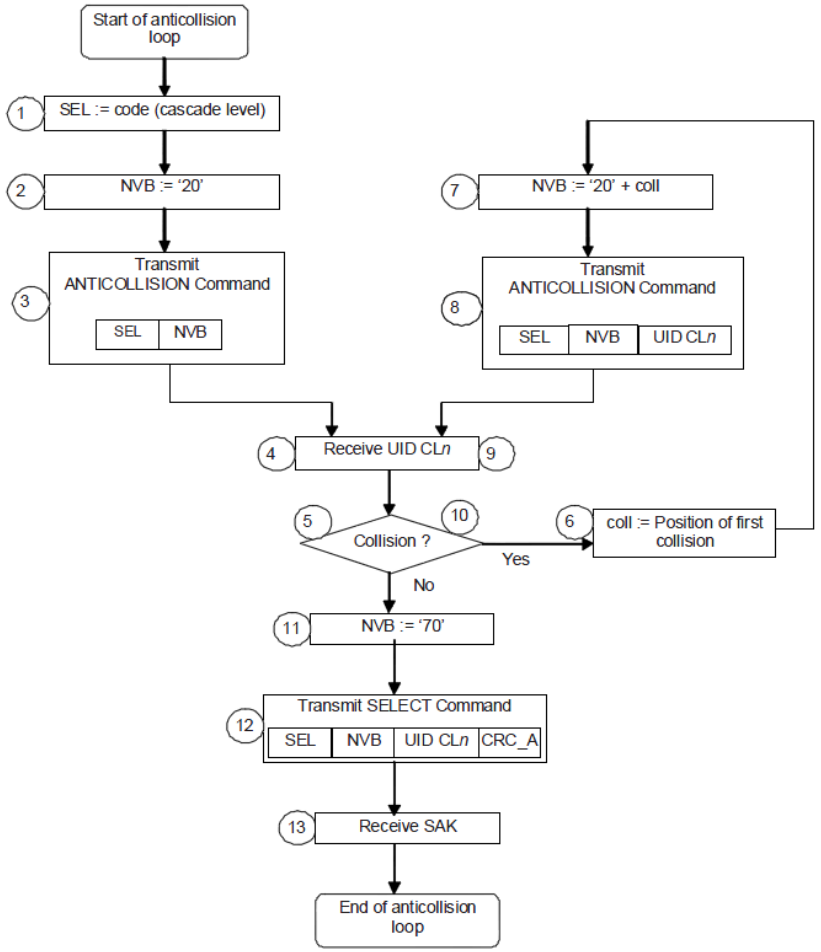


Figure 10 — Anticollision loop, flowchart for PCD

6.5.3 Anticollision and Select

6.5.3.1 Anticollision loop within each cascade level

The following algorithm shall apply to the anticollision loop:

Step 1	The PCD shall assign SEL with the code for the selected anticollision cascade level.
Step 2	The PCD shall assign NVB with the value of '20'. NOTE This value defines that the PCD will transmit no part of UID CL*n*. Consequently this command forces all PICCs in the field to respond with their complete UID CL*n*.
Step 3	The PCD shall transmit SEL and NVB.
Step 4	All PICCs in the field shall respond with their complete UID CL*n*.
Step 5	If more than one PICC responds, a collision may occur. If no collision occurs, steps 6 to 10 shall be skipped.
Step 6	The PCD shall recognize the position of the first collision.
Step 7	The PCD shall assign NVB with a value that specifies the number of valid bits of UID CL*n*. The valid bits shall be part of the UID CL*n* that was received before a collision occurred followed by a (0)b or (1)b, decided by the PCD. A typical implementation adds a (1)b.
Step 8	The PCD shall transmit SEL and NVB, followed by the valid bits.
Step 9	Only PICCs of which the part of UID CL*n* is equal to the valid bits transmitted by the PCD shall transmit their remaining bits of the UID CL*n*.
Step 10	If further collisions occur, steps 6 to 9 shall be repeated. The maximum number of loops is 32.
Step 11	If no further collision occurs, the PCD shall assign NVB with the value of '70'. NOTE This value defines that the PCD will transmit the complete UID CL*n*.
Step 12	The PCD shall transmit SEL and NVB, followed by all 40 bits of UID CL*n*, followed by CRC_A.
Step 13	The PICCs which UID CL*n* matches the 40 bits shall respond with their SAK.
Step 14	If the UID is complete, the PICC shall transmit SAK with cleared cascade bit and shall transit from READY state to ACTIVE state or from READY* state to ACTIVE* state.
Step 15	The PCD shall check if the cascade bit of SAK is set to decide whether further anticollision loops with increased cascade level shall follow.

If the UID of a PICC is complete and known by the PCD, the PCD may skip step 2 - step 10 to select this PICC without performing the anticollision loop.

ISO standards- card collision

- Unlike EMV, ISO specifies no termination in the case of a collision. Instead, a race condition is created in which depending on the implementation of the terminal, and the UIDs of the cards available in the field one card would be selected.

Experiments on contactless terminals

- Testing multiple cards on different terminals in different metro stations

Card	Tech.	UID size	UID0 Hex	UID0 Binary (LSB)	ISO winner
TSB visa debit- Card 1	A	4	0x35	(10101100)b	✓
TSB visa debit- Card 2	A	4	0x65	(10100110)b	✗
Barclays visa debit- Card 1	A	4	0xE7	(11100111)b	✓
Barclays visa debit- Card 2	A	4	0x87	(11100001)b	✗
barclaycard Platinum visa - Card 1	A	4	0x67	(11100110)b	✗
barclaycard Platinum visa- Card 2	A	4	0xDF	(11111011)b	✓
Nexus 5	A	4	x08	(00010000)b	✗

Cards' information, LSB: Least Significant Bit.

Results don't match EMV/ISO

No.	POS	Issuing bank	Facing card to reader	Result	Msg
1	MS 1, POS 1	TSB	Card 1	No operation	
2	MS 1, POS 1	TSB	Card 2	No operation	
3	MS 2, POS 1	TSB	Card 1	No operation	
4	MS 2, POS 1	TSB	Card 2	No operation	
5	MS 1, POS 2	TSB	Card 1	No operation	
6	MS 1, POS 2	TSB	Card 2	Card 1 won	msg1
7	MS 1, POS 2	TSB	Card 1	Card 2 won on 2nd try	msg1
8	MS 2, POS 2	TSB	Card 2	Card 1 won	
9	MS 2, POS 2	TSB	Card 1	No operation	
10	MS 2, POS 2	TSB	Card 1	No operation	
11	MS 1, POS 2	Barclays	Card 2	Card 1 won	
12	MS 1, POS 2	Barclays	Card 1	Card 2 won	
13	MS 1, POS 2	Barclays	Card 2	Card 1 won	msg1
14	MS 1, POS 2	Barclays	Card 1	Card 2 won	
15	MS 2, POS 1	Barclays	Card 2	Card 1 won	
16	MS 2, POS 1	Barclays	Card 1	Card 2 won	msg1
17	MS 2, POS 1	Barclays	Card 2	Card 1 won	msg1
18	MS 1, POS 3	barclaycard	Card 2	Card 1 won	
19	MS 1, POS 3	barclaycard	Card 1	Card 1 won	
20	MS 1, POS 3	barclaycard	Card 2	Card 1 won	
21	MS 1, POS 3	barclaycard	Card 1	Card 1 won	
22	MS 2, POS 2	barclaycard	Card 2	Card 1 won	
23	MS 2, POS 2	barclaycard	Card 1	Card 1 won	
24	MS 1, POS 1	barclaycard	Card 2	Card 1 won on 2nd try	msg2
25	MS 1, POS 1	barclaycard	Card 1	Card 1 won	
26	MS 2, POS 3	barclaycard	Card 2	Card 1 won	
27	MS 2, POS 3	barclaycard	Card 1	Card 1 won	

The results of putting card pairs in the race condition. MS stands for Metro Station. In the case of No operation, the cards were presented 3 times to the POS for the same transaction. msg1: "Only present one card", msg2: "Card read failed".

Attack based on this inconsistency

- A malicious app spying on user's contactless transactions

flip wallet

Opanable cover

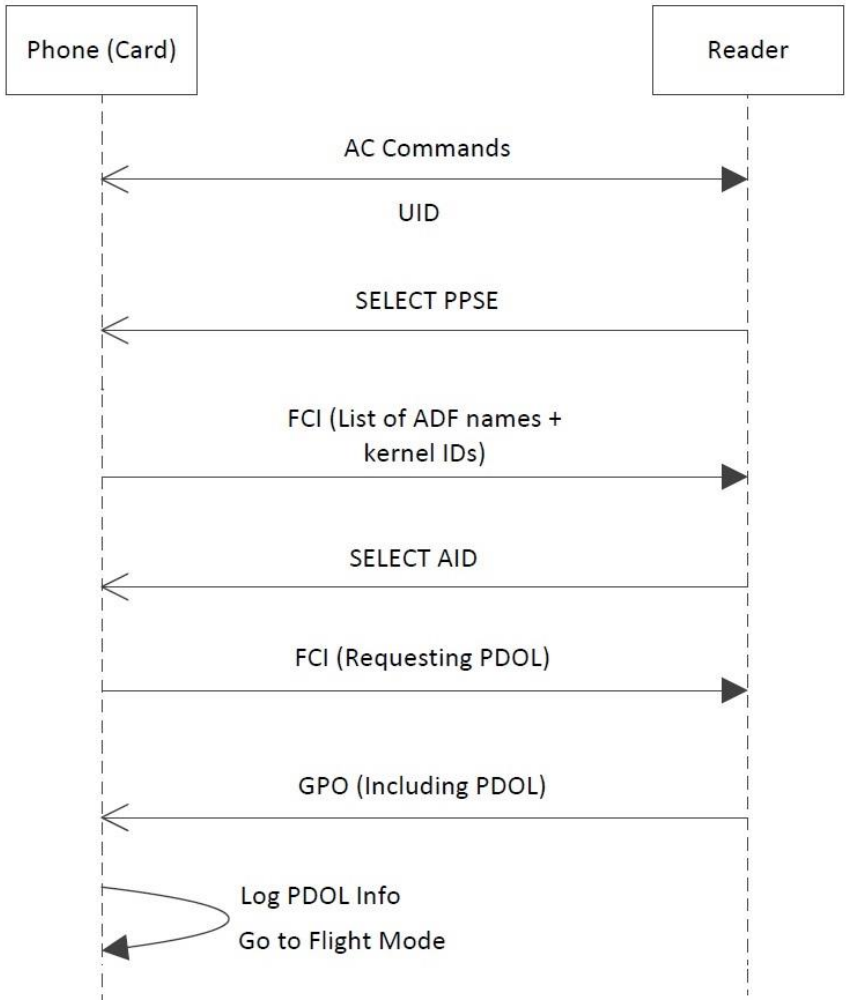
transparent cover

back cover/stand

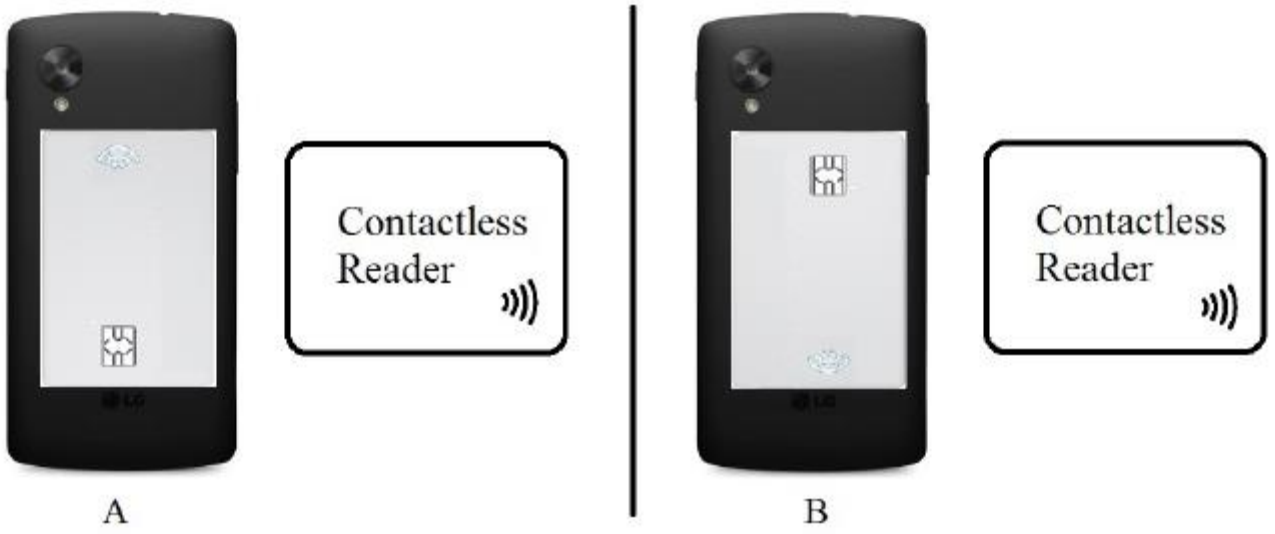
sticker cover

Attack Design

- Simulating a card on Android HCE
- Registering a Visa card AID
- Requesting Processing Options Data Object List (PDOL)
- A Get Processing Option (GPO) is returned
- Includes the Terminal Transaction Qualifiers (TTQ), Unpredictable Number, Amount, Authorised, Transaction Currency Code, and other tags



Experiments



A: the NFC chipset was down B: the NFC chipset was up

Phone Wins in 66% of cases

No.	Card	Terminal	Position	Winner	Msg
22	Barclays 1	MS 1, POS 1	A	Phone	
23	Barclays 1	MS 1, POS 1	A	Phone	
24	Barclays 1	MS 1, POS 1	A	Phone, 2nd try	msg1
25	Barclays 1	MS 1, POS 1	A	Phone	
26	Barclays 1	MS 1, POS 1	A	Phone	
27	Barclays 1	MS 1, POS 1	A	Phone	
28	Barclays 1	MS 1, POS 1	B	Card	
29	Barclays 1	MS 1, POS 1	B	Phone	
30	Barclays 1	MS 1, POS 2	B	Card, 2nd try	”msg1”
31	Barclays 1	MS 1, POS 2	B	Phone	
32	Barclays 1	MS 1, POS 2	B	Card	
33	Barclays 1	MS 1, POS 2	B	Phone	
34	Barclays 2	MS 1, POS 2	A	Phone	
35	Barclays 2	MS 1, POS 2	A	Phone	
36	Barclays 2	MS 1, POS 2	A	Phone	
37	Barclays 2	MS 1, POS 2	A	Phone	
38	Barclays 2	MS 1, POS 2	A	Card	”msg2”
39	Barclays 2	MS 1, POS 2	B	Card	”msg2”
40	Barclays 2	MS 1, POS 2	B	Card, 2nd try	”msg1”
41	Barclays 2	MS 1, POS 2	B	Phone	
42	Barclays 2	MS 1, POS 1	B	Card	
43	Barclays 2	MS 1, POS 1	B	Card	
44	Barclays 2	MS 1, POS 1	B	Phone, 2nd try	”msg1”

Results of experiment A for Barclays cards, msg1: “Card read failed”, msg2: “Only present one card”.

PDOL

- Phone:
  - PDOL tag: ‘9F38’
  - Amount tag: ‘9F02’
  - Date tag: ‘9A’
- Reader:
  - PDOL tag: ‘83’
  - Amount: ‘000000000080’ (0.80 pence)
  - Date: ‘160523’ (2016 May 23)

Sender	APDU	Command
Terminal	00A404000E325041592E5359532E E444446303100	SELECT PPSE
Phone	6F3C840E325041592E5359532E44 44463031A52ABF0C2761254F07A0 0000000310108701015010424152 434C4159434152442056495341BF 6304DF2001809000	FCI
Reader	00A4040007A0000000031010 00	SELECT AID
Phone	6F4B8407A0000000031010A54050 10424152434C4159434152442056 4953418701019F38189F66049F02 069F03069F1A0295055F2A029A03 9C019F37045F2D02656EBF0C089F 5A0531082608269000	FCI including PDOL request
Terminal	80A8000023832130000000000000 00008000000000000826000000 00000826160523001612673900	GPO including PDOL data

Exchanged APDUs of the PDOL experiment

Conclusion

- Summary:
  - Studied card collision problem, EMV, ISO, Implementation in practice
  - Found inconsistency
  - Preformed an attack on privacy of transactions (amount, date)
- More attacks:
  - Merchant information for Mobile payments
- Solutions:
  - Implementation to match EMV
  - EMV to protect private info
  - Mobile platforms to rethink about the access permission of sensors

Questions!