



OWASP
Open Web Application
Security Project

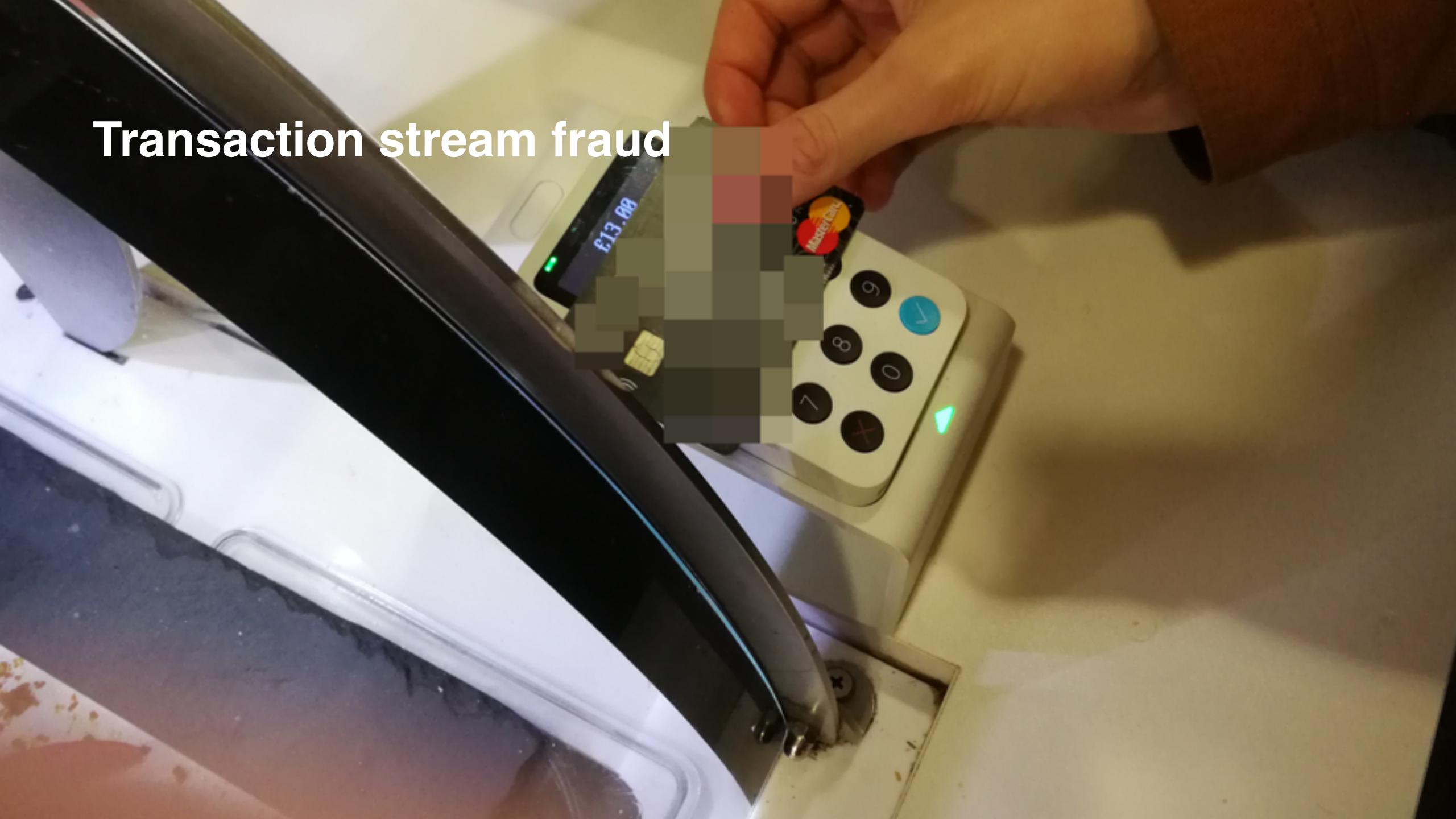
Hack in, Cash out

Hacking and Securing Payment Technologies

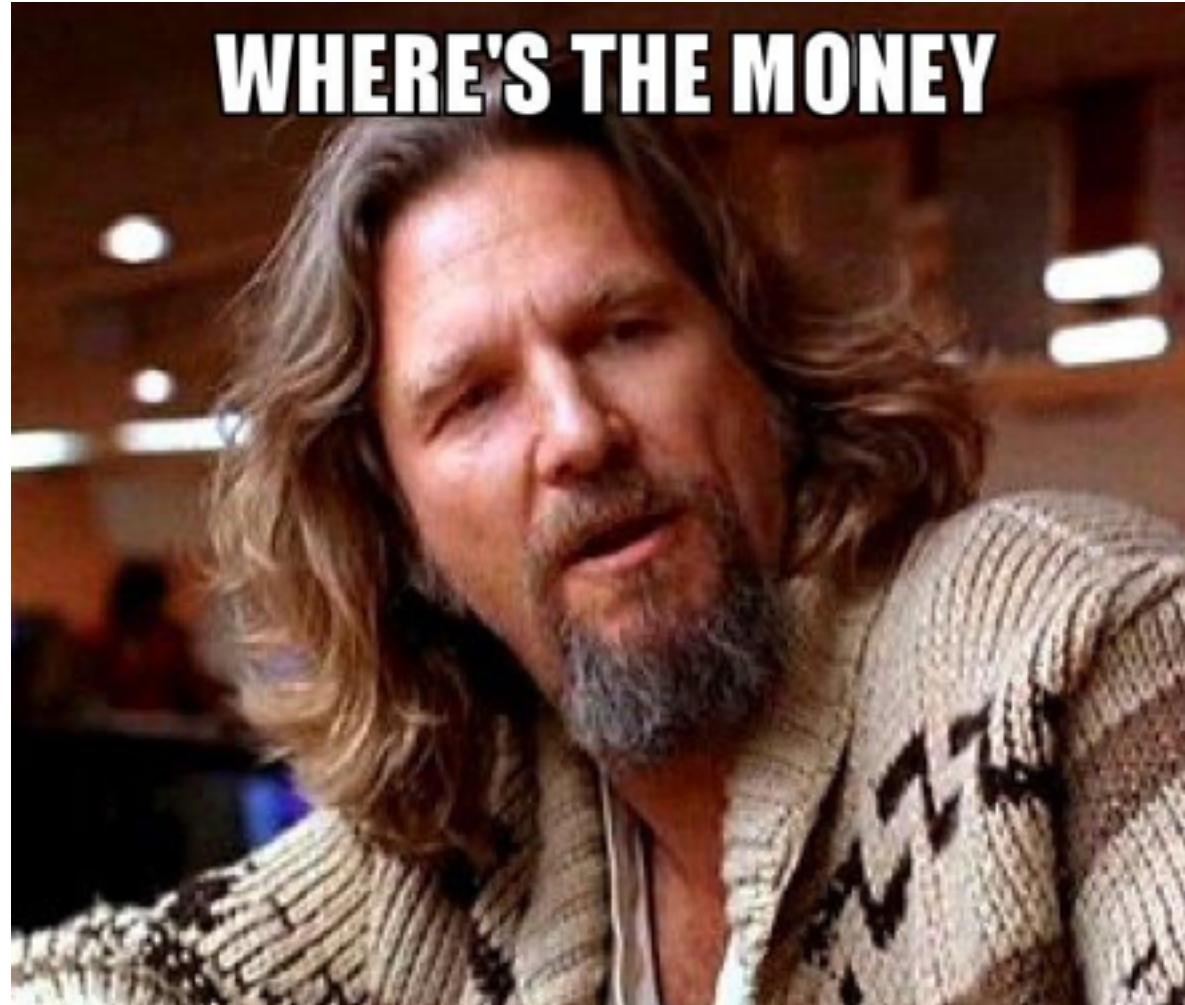
Tim Yunusov

POSITIVE TECHNOLOGIES

Transaction stream fraud



Main question of the payment pentest



Good pentest



Bad pentest



Get money from the bank



From our own accounts



Decisions, decisions...

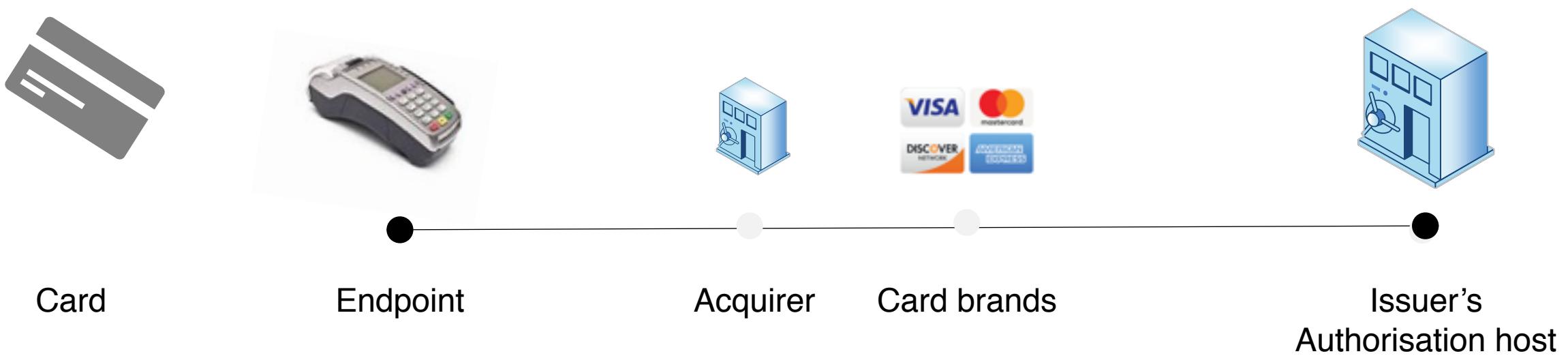


4 accounts in 2018
4 accounts in 2019



Prepared by: Arif Sidiqi

Card payment processing



Endpoints

	ATM	POS	Online
Money	+	+	+
Card's data	+	+	+
Card's testing	Limited	+	+
Card's attacks	Limited	+	Limited



Most ATMs can be hacked in under 20 minutes

Experts tested ATMs from NCR, Diebold Nixdorf, and GRGBanking.



By [Catalin Cimpanu](#) for [Zero Day](#) | November 16, 2018 -- 05:30 GMT (05:30 GMT) | Topic: [Security](#)

black hat
USA 2018
AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS

Blackbox is dead –
Long live Blackbox!

Vladimir Kononovich
Aleksey Stennikov

ptsecurity.com

@BHUSA / #BLACKHAT EVENTS

POSITIVE TECHNOLOGIES



@A1ex_S

@groke1105

@ivachyou

@L_AGalloway



Terminal Simulator

Testing Tomorrow's Transactions Today

Welcome

This site has been created to allow you to obtain the latest versions of our Terminal Simulator software, which requires a PC/SC card reader. If you don't have such a reader, you can order a simulator kit, that will include a dual interface (contact and contactless) reader, and the associated software on CD. Please go ahead and register as a user on this site, and then you will be able to download or order the products that are listed below.

Featured Products



Activation Extension
2020
Extension of
activation to January
2020
[View more details](#)

[View more details](#)



<https://www.terminalsimulator.com/>

uire a PC/SC card reader. If you don't have such a reader, you can order a or order the products that are listed below.

```

Terminal Simulator

Tag : 91 [Issuer Authentication Data]
Length: 0A
Data : 7457472F641878770000
ARPC1: 7457472F64187877
ARPC Response code: 0000
Online Response is DECLINED
=====

Transaction time = 5170ms (terminal: 3484ms APDU: 1686ms)

Generating AC Command
=====

COOL2 = 9104840295059F37049F8C0B
COOL2 Data = 7457472F641878770000100000000000003080313990e3bf866626fb2
+ Finished generating AC command
=====

+ sending 2nd GENERATE AC command

--> Command :
CLA INS P1 P2 LC LE
00 AE 00 00 1D 00

74 57 47 2F 64 18 78 77 00 00 00 01 00 00 00 00 00 00 00 two/d. [w.....
00 30 80 31 39 90 03 88 F6 06 26 EF B2 .0.39...F6...
<-- Response: (SW1-SW2) 9000 (Length) 28
77 29 9E 27 01 00 9E 36 02 05 ED 9E 26 08 F9 38 w. ....6..$.
BF 34 1E 57 80 56 9E 10 13 01 10 20 9E 03 24 04 ..4..W.V.....$.
09 90 B3 09 00 00 03 40 00 00 FF .....$.

Transaction time = 176 ms

Tag : 77 [Response Message Template format 2]
Length: 29
| Tag : 9E27 [cryptogram information data]
Length: 01
Data : 00
Tag : 9E36 [Application Transaction Counter (ATC)]
Length: 02
Data : 05ED
Tag : 9E20 [Application cryptogram]
Length: 08
Data : 93180F3411576056
Tag : 9E10 [Issuer Application Data]
Length: 12
Data : 0110209003240400908700000003480000FF

+ GENERATE AC processed ok
    CID          = 00 - AAC
    ATC          = 05ED
    Cryptogram   = 93180F3411576056

```



POS+RCE – is the instrument

- EMV/NFC core real implementation
 - May contain a lot of bugs
- Real payment process workflow
 - Payment packet
 - Configurations (limits, etc)
 - Offline authentication and risk management



Example of the payment packet

```
{"invoiceId": "INV2-[REDACTED]", "dateTime": "2019-03-18T11:05:58+0000", "card": {"reader": {"vendor": "[REDACTED]", "readerSerialNumber": "10552290", "dev": "[REDACTED]", "inputType": "contactless_chip", "emvData": "500a4d6173746572436172645f24032109305f280208265f2a0208265f340100820219808407a0000000041010950500000080009a031903189c01209f0206000000000001009f030600000000000009f0607a00000000410109f090200029f10120110800003220800000000000000000000ff9f120a4d6173746572436172649f1a0208269f1c0831323334353637389f1e0831303535323239309f2608cad7779c1aa2a3c99f2701009f33030008089f34031f03029f3501229f360204429f3704aaaaaaaaadfd280100df30020201dfaef022097c2508543007dfe18bbdd076c76d61dd813094c12e6ac83855232ae43caa05edfae030affff9802840f88200168dfaef5a08537590fffff5611"}}}
```

BER encoding

- TLV – Tag Length Value

Example

- AA0105 [hex]
- Tag – AA
- Length – 1 byte
- Value - 05

00 69 00 43 00 EA 01
00 01 0D 03 00 12 06
00 A7
00 20
01
03
00 33
00 53
00 01 \Number of TLVs - top level
29 FF 00 4D \Parent TLV
Nested [] 2A 0E 00 04 D0 D1 2B 37
TLVs [] 2A 01 00 41\Length includes all nested TLVs
Nested [] 2A 03 00 01 00
TLVs [] 2A 07 00 04 00 00 13 98
Nested [] 2A 0A 00 02 00 14
TLVs [] 2A 02 00 13 \Length includes next 3 TLVs
Nested [] 2A 08 00 02 00 02
TLVs [] 2A 09 00 01 02
Nested [] 2A 0B 00 04 00 00 1F 40
2A 02 00 13 \Length includes next 3 TLVs
Nested [] 2A 08 00 02 01 65
TLVs [] 2A 09 00 01 32
2A 08 00 04 00 00 1F 40

Example of the payment packet

50 (application label) MasterCard

5F24 (card expiry) 210930

5F28 (issuer country code) GBR (United Kingdom)

5F2A (terminal currency code) GBP (Pound Sterling)

5F34 (PAN sequence number) 00

82 (AIP - Application Interchange Profile) ↗

1000 (Byte 1 Bit 5) Cardholder verification is supported

0800 (Byte 1 Bit 4) Terminal risk management is to be performed

0100 (Byte 1 Bit 1) CDA supported

0080 (Byte 2 Bit 8) EMV and Magstripe Modes Supported

84 (dedicated file name) A0000000041010

95 (TVR - Terminal Verification Results) ↗

000000080000 (Byte 4 Bit 8) Transaction exceeds floor limit

9A (transaction date) 190318

9C (transaction type) 20

9F02 (amount authorized) 000000000100

9F03 (amount other) 00000000000000

9F06 (application id) A0000000041010

9F09 (terminal application version number) 0002

9F10 (issuer application data) ↗

Key Derivation index 01

Cryptogram version number 10

Card verification results ↗

Byte 1 Bit 8 = 1, Byte 1 Bit 7 = 0 Second Generate AC not requested

Byte 1 Bit 6 = 0, Byte 1 Bit 5 = 0 AAC Returned in First Generate AC

Byte 3 Bits 8-5 Right nibble of Script Counter = 0

Byte 3 Bits 4-1 Right nibble of PIN Try Counter = 3

Byte 4 Bit 6 = 1 Offline PIN Verification Not Performed

Byte 4 Bit 2 = 1 Domestic Transaction

Byte 5 Bit 4 = 1 Go Online On Next Transaction Was Set

DAC/ACC Dynamic Number 2 Bytes 0000

Plaintext/Encrypted Counters 00000000000000FF

9F12 (application preferred name) MasterCard

9F1A (terminal country code) GBR (United Kingdom)

9F1C (terminal id) 12345678

9F1E (terminal serial number) 10552290

9F26 (application cryptogram) CAD7779C1AA2A3C9

9F27 (cryptogram information data) AAC (Application Authentication Cryptogram - Declined)

9F33 (terminal capabilities) ↗

000800 (Byte 2 Bit 4) No CVM Required

000008 (Byte 3 Bit 4) CDA

9F34 (CVM Results - Cardholder Verification Results) ↗

1F No CVM required

03 If terminal supports CVM

02 Successful

9F35 (terminal type) 22

9F36 (ATC - application transaction counter) 1090

9F37 (unpredictable number) A3D751EA

DF28 (?) 00

DF30 (?) 0201

DFAE02 (?) 97C2508543007DFE188BDD076C76D61DD813094C12E6AC83855232AE43CAA05E

DFAE03 (?) FFFF9802840F88200168

DFAE5A (?) 537590FFFFFF5611

<https://tvr-decoder.appspot.com>

PAN/Track2/Expiry date

Transaction date and time

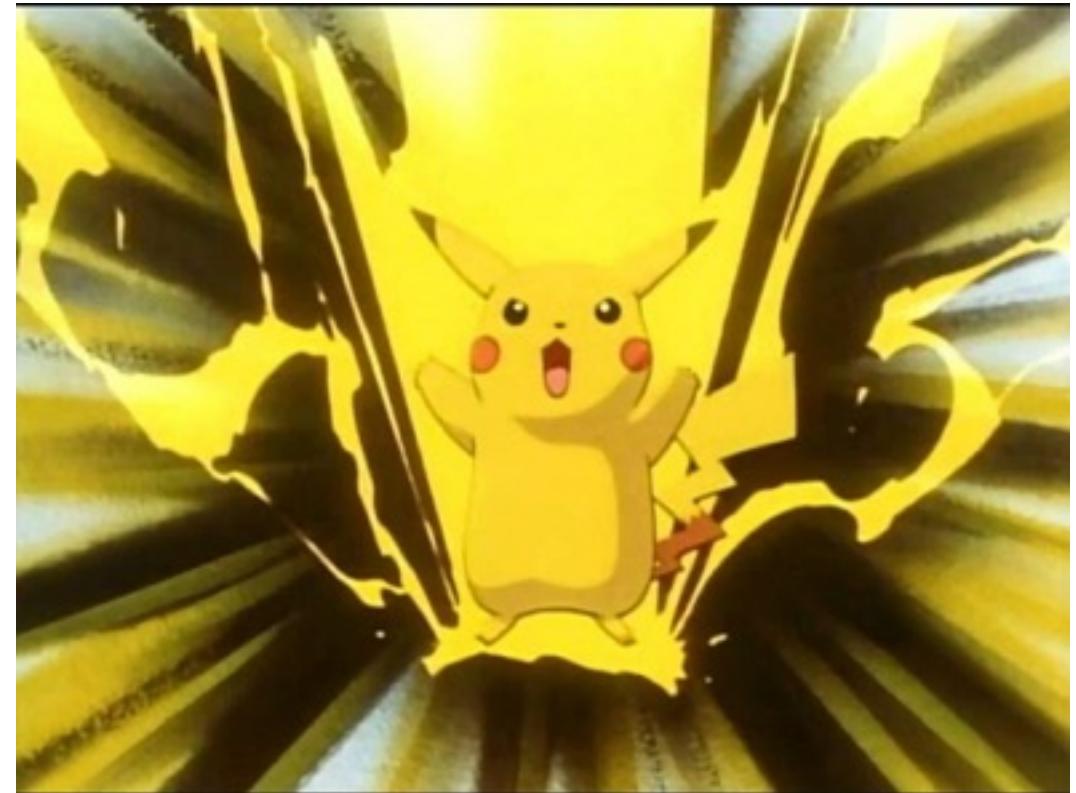
Amount and currency

Type of the operation (payment, cashback, refund, other)

Type of the cryptogram, cardholder verification method

Attacks

- Refund/reverse attacks
- Chip & PIN attacks
- Card testing



72,811 views | Nov 23, 2015, 06:40am

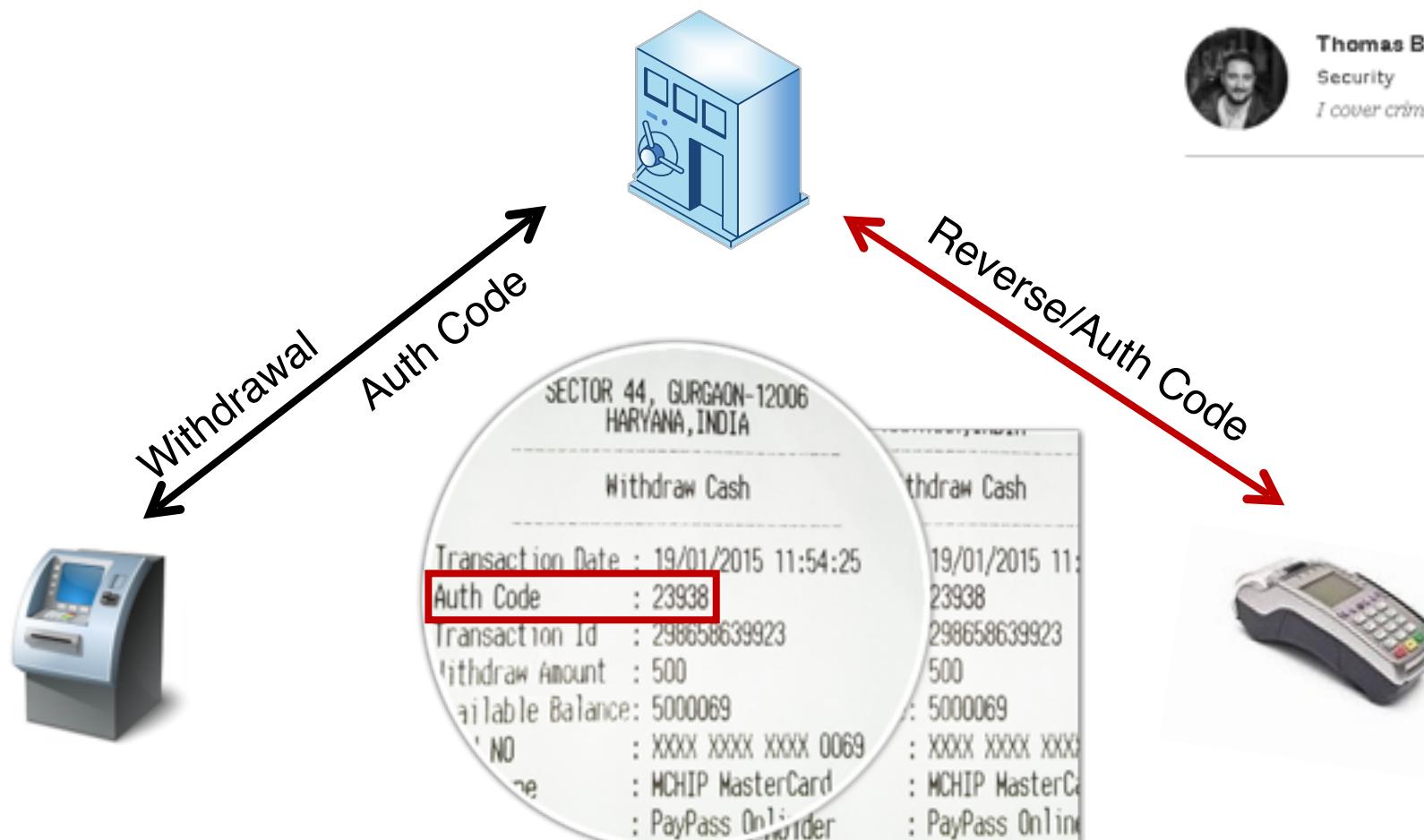
Reverse attacks

Criminals Steal \$4 Million In Cash With Novel 'Reverse ATM' Attack

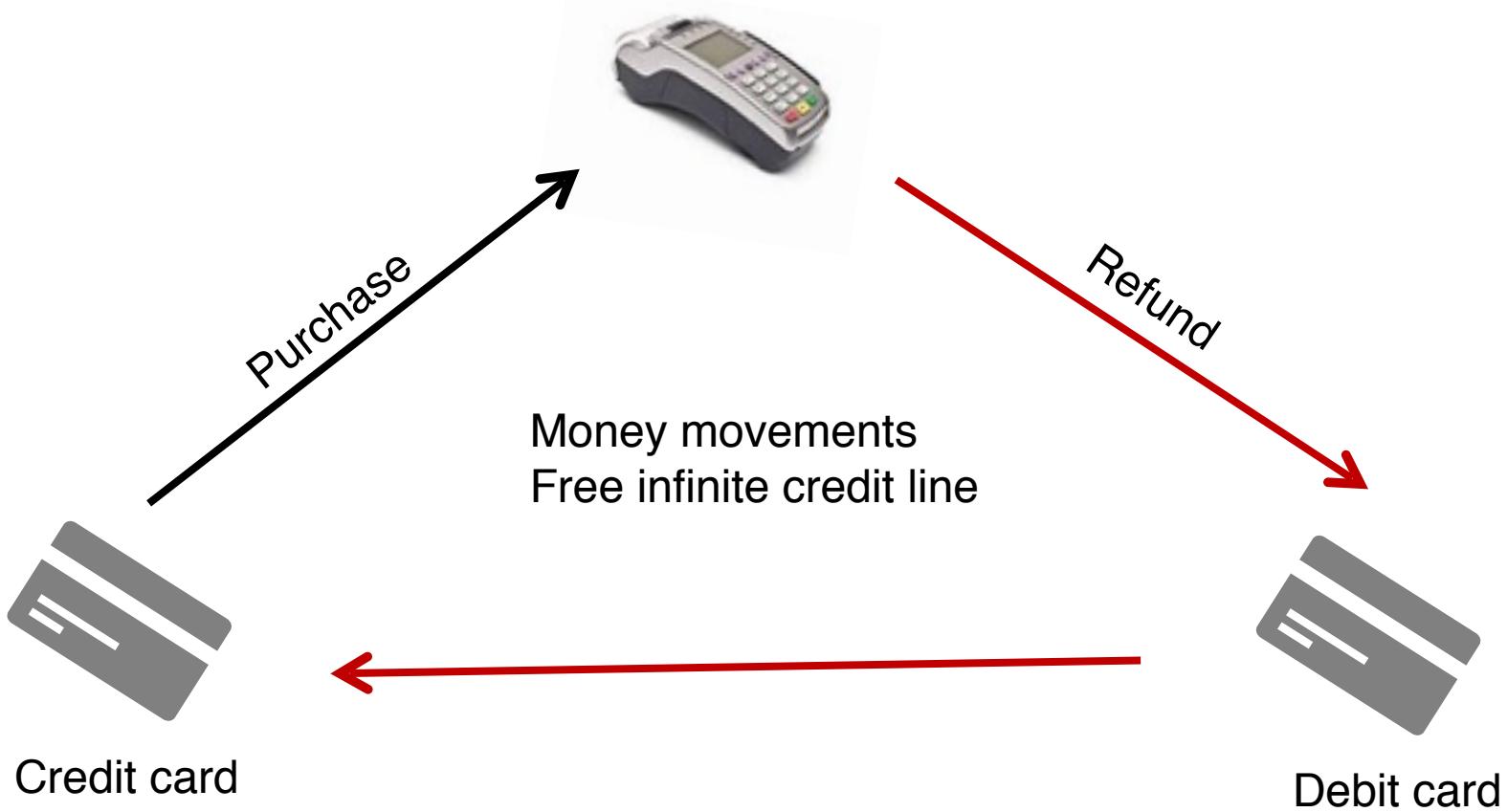


Thomas Brewster Forbes Staff

Security

I cover crime, privacy and security in digital and physical forms.

Refund attacks



Chip & PIN is still broken

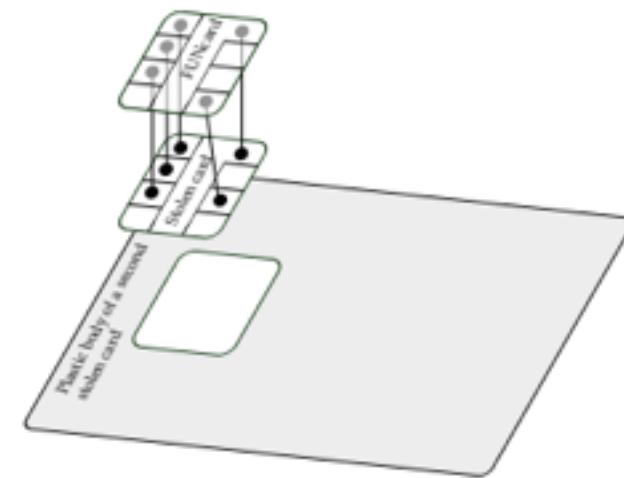
- 2005 University of Cambridge, <https://murdoch.is/papers/cl05chipandpin.pdf>
- 2010 Inverse Path (F-Secure) / Aperture Labs
<https://cansecwest.com/csw11/Chip%20&%20Pin%20-%20Barisani%20&%20Bianco.pdf>
 - Intercept PIN (ICC plaintext PIN verification)
 - Make transactions without PIN knowledge (“PIN OK” attack)
 - Downgrade to chip&signature

Chip & PIN is still broken

- CVM list – cardholder verification method list
 - CVM list is defined on the card
 - CVM List provides the terminal with four pieces of information on how an issuer wishes the cardholder to be verified:
 - CVM method (in priority)
 - Conditions of use
 - What if the CVM method is failed
 - Encrypted PIN if supports, then Unencrypted PIN if supports, the signature, than cancel
 - <https://www.spotterswiki.com/emv/cardsearch.php>
 - <https://tvr-decoder.appspot.com>
- Offline data authentication – when POS checks that card and it's data were genuine: SDA, DDA, **CDA**

When hackers come

- 2011, France <https://eprint.iacr.org/2015/963.pdf>
 - 40 cards
 - PIN-OK additional chip
 - 7000 transactions
 - 680,000 USD



Chip & PIN is still broken

- 2019, Europe
 - PIN interception, “PIN OK” attack, chip&signature downgrading
- Why?
 - “Nowadays CVM is signed” (c) Inverse Path - **CDA**
 - Weak CVM Lists: PIN Online if unattended, PIN Offline elsewhere
 - Visa cards do not provide Offline Data Authentication
 - Card supports (DDA,CDA), terminal supports (DDA,CDA):
 - Terminal choose DDA
 - Terminal goes online if the offline authentication is failed

Card testing

- Balance testing for stolen cards
- <https://www.zdnet.com/article/hackers-abuse-magento-paypal-integration-to-test-validity-of-stolen-credit-cards/>

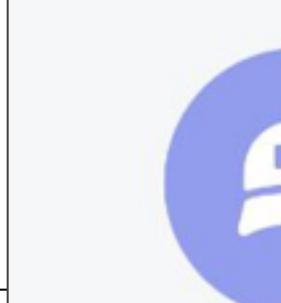
Payment methods > Add payment method

Add a payment method

Add credit or debit card

Card number
#

MM / YY
CVC

	scupsm.com	-47,99 \$
	EXSBILLING.COM	-7,22 \$
	Google Services	29 Jun, 11:25
	Google Services	26 Jun, 10:50, Please unfreeze your card to make this transaction
	Google Services	26 Jun, 10:50, Please unfreeze your card to make this transaction

When hackers come first

- Nov, 2016, 40,000 accounts, 9,000 successfully

Tesco Bank says attack cost it £2.5m and hit 9,000 people

🕒 8 November 2016

f t m e Share



Was it hacked?

Tesco did not use the "H" word in its statement and in interviews

Card testing

- 1 Dec 2016, Newcastle University
- https://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf
- Consecutive enumeration:
 - BIN (public DB)
 - PAN (online banking registration)
 - Expiry Date (refund, recipient of funds)
 - CVV (regular payment)
 - Postcode for AVS (different error)

TABLE I. VARIATION IN PAYMENT SECURITY SETTINGS OF ONLINE PAYMENTS WEBSITES

Number of attempts allowed	Sites with 2 fields (guess expiry date)	Sites with 3 fields (guess CVV2)	Sites with 4 fields (guess address postcode)	Sites with 3D Secure (safe from attack)	Total
0 to 5	2	23	2	-	27
6 to 10	20	238	18	-	276
11 to 50	2	28	3	-	33
Unlimited	2	2	2	-	6
3D Secure	-	-	-	47	47
Total	26	291	25	47	389

Card testing

- 1 Dec 2016, Newcastle University
- https://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf
- Consecutive card testing
 - PAN
 - Expiry Date (refund, recipient of funds)
 - CVV (regular payment)
 - Postcode for AVS (different error)

FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack

Press Releases | Published: 01/10/2018 | Last updated: 01/10/2018

URITY SETTINGS OF ONLINE
S

	allowed	(guess expiry date)	(guess CVV2)	(guess address postcode)	Sites with 3D Secure (safe from attack)	Total
0 to 5	2	23	2	-	27	
6 to 10	20	238	18	-	276	
11 to 50	2	28	3	-	33	
Unlimited	2	2	2	-	6	
3D Secure	-	-	-	47	47	
Total	26	291	25	47	389	

Card testing

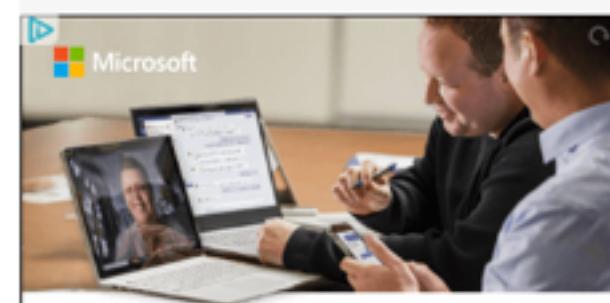
- July 2018, Monzo

▷ <https://www.theguardian.com/money/2018/jul/07/heres-how-scammers-get-away-with-it>

Transaction attacks

On the Monday morning I visited Monzo's offices, just 12 hours earlier there had been a “pan enumeration” attack on its computer systems. This is where fraudsters, often based overseas, bombard a bank’s computers, trying to guess passwords and logins, or attempting to do transactions by generating card expiry dates and three-digit CVCs (card verification codes) in the hope that some might break through.

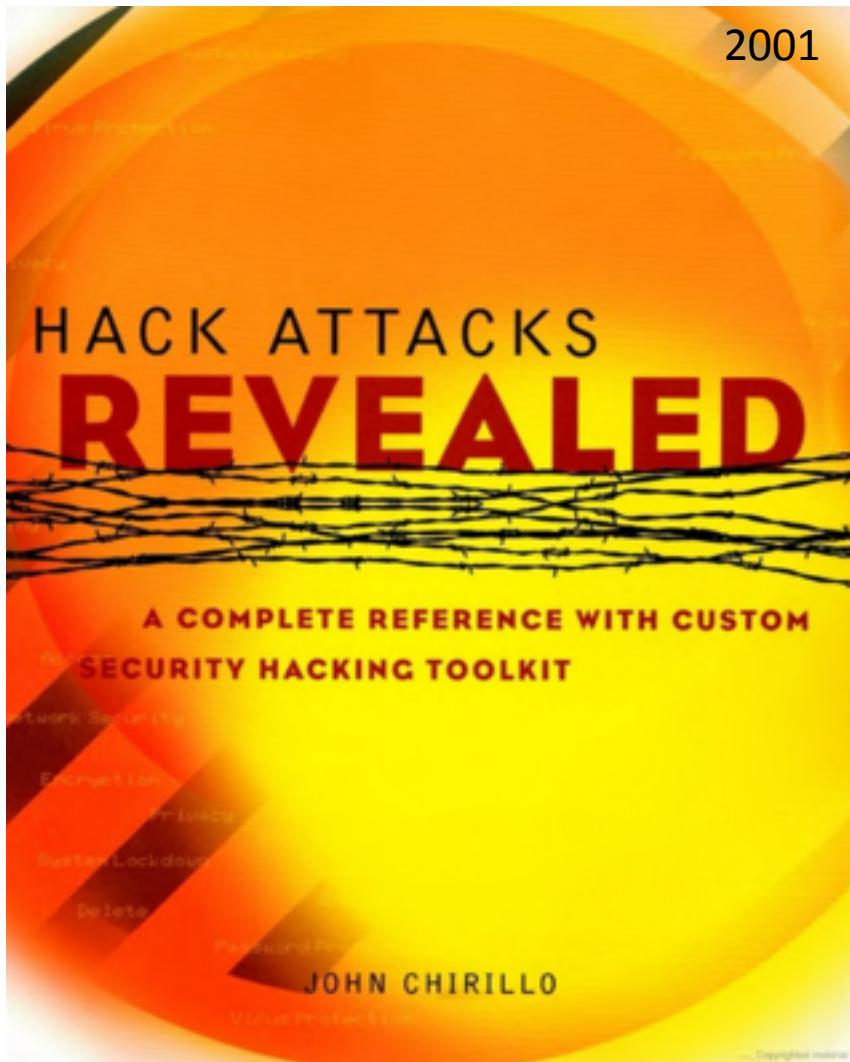
Advertisement



Meet the hub for teamwork in
Office 365 Business Premium

[CLICK HERE →](#)

Rounding



ZeroNights 2013



Practical exploitation of rounding vulnerabilities in internet banking applications

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com

Hacker News new | past | comments | ask | show | jobs | submit

▲ Round error issue - produce money for free on itBit bitcoin exchange (hackerone.com)
70 points by waffle_ss on Mar 3, 2017 hide | past | web | favorite | 60 comments

Rounding

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.0153; 2) == 0.02 GBP
- 0.02 GBP => float(0.026; 2) == to 0.03 USD
- Profit = 0.01 USD

Rounding

- 1 GBP = 1,30 USD
- 0.02 USD => float(0)
- 0.02 GBP => float(0)
- Profit = 0.01 USD



Rounding

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.0153; 2) == 0.02 GBP
- 0.02 GBP => float(0.026; 2) == to 0.03 USD
- Profit = 0.01 USD

x10,000

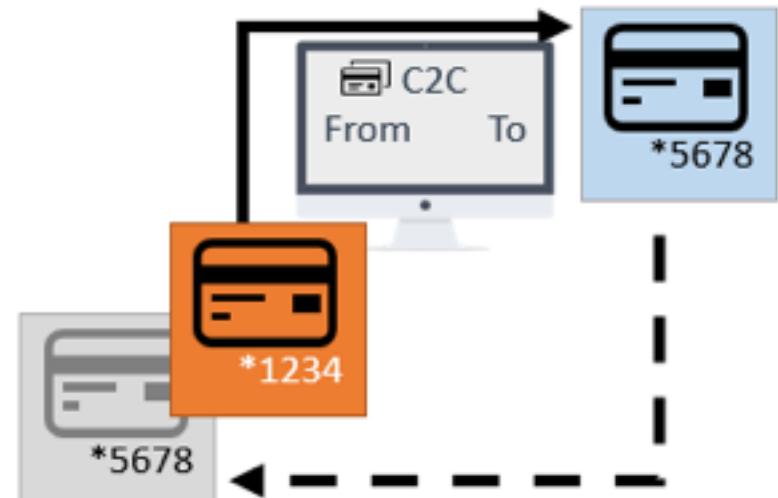
- OTP bypass
- Antifraud bypass
- Don't need to do everything manually

Stat

- Maximum amount per project – \$463,843 in 3 days (in live)
- In 2019 – 8/8 banks in Europe were *potentially* vulnerable to rounding,
one bank has confirmed the vulnerability

How to lose money during payment research

- Startup, which “allows you to spend money from any of your accounts using just one * Card” - *1234
- Connect any of your cards in the mobile app
- When you pay from the card *1234,
money will be withdrawn from the card you’ve chosen and connected (*5678)
- What if we will use Card2Card and send
From *1234 To *5678
- Just a regular transaction for *5678
- We will get a cashback!

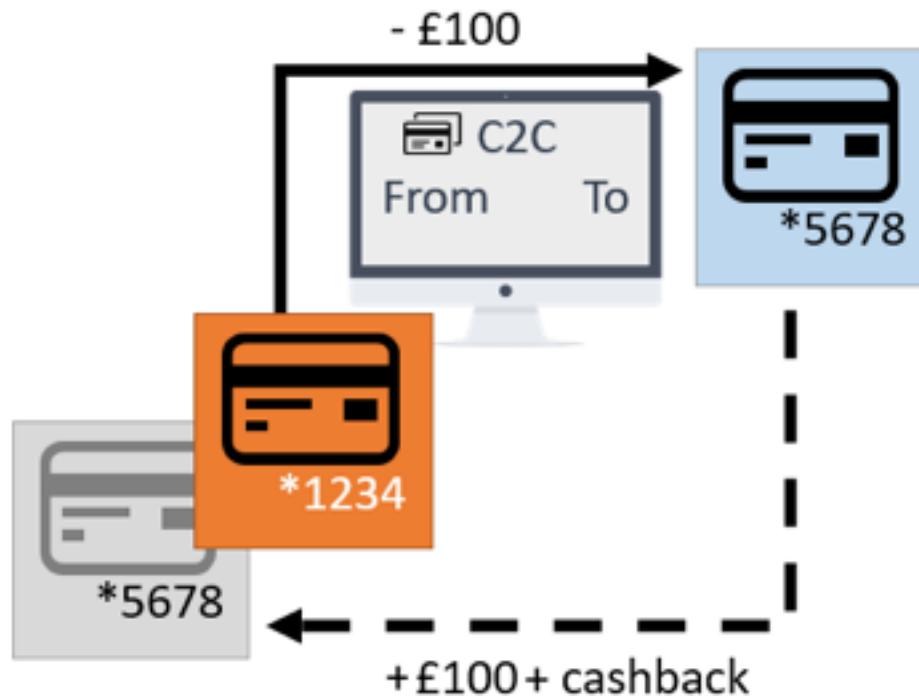


How to lose money during payment research

- Send £100
- Money were withdrawn twice!
- Waited 5+ days
- Used 3 different card2card services
- Used 3 different cards, connected in the app

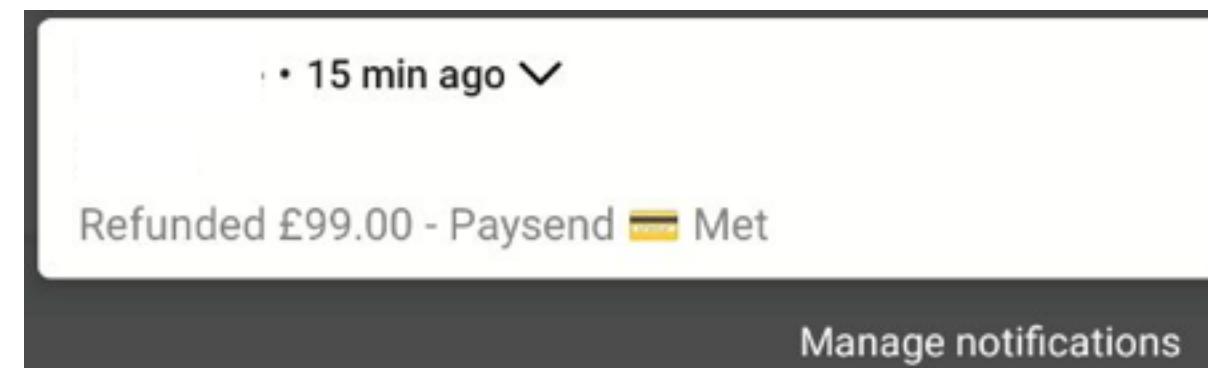
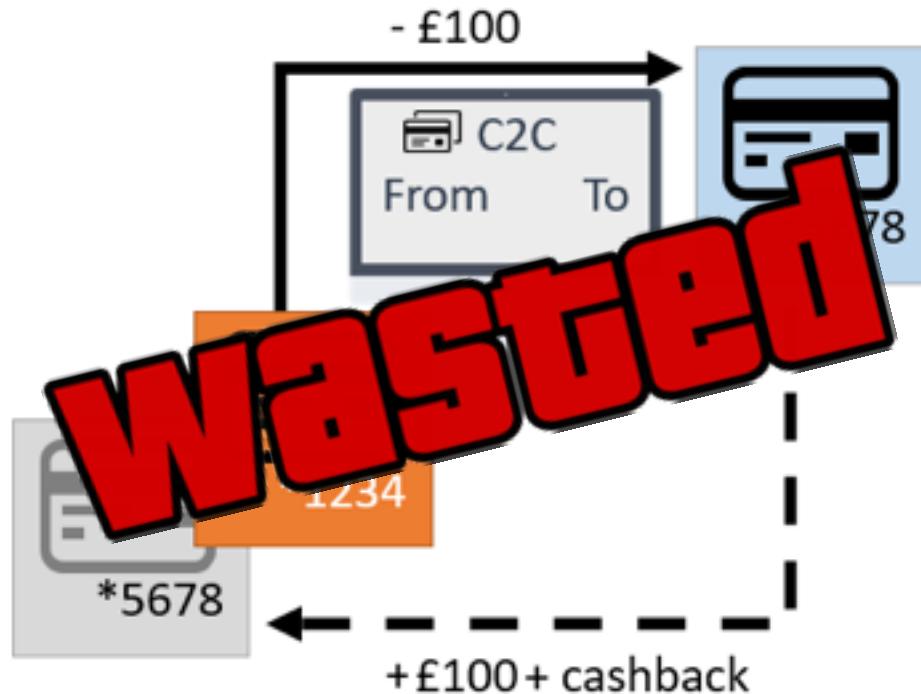
 Waitrose 12 Apr, 20:06	- £25.48	 We have received your payment! We have received your payment, your money transfer is now being processed.
 paysend 12 Apr, 16:33	- £99	Send amount: 5.00 GBP to Timur Iunusov in United Kingdom Receive amount: 5.00 GBP Fee: 0.00 GBP Total to pay: 5.00 GBP Delivery method: Card Deposit Delivery details: Card Number: *5611 Card Type: mastercard Cardholder Name (as printed on card): Iunusov Timur Payment method: Bank Card Payment reference:
 Paysend 12 Apr, 16:27	- £100	Today
 Send Money 24 Ltd Saturday 15th June	5.00	
 Sendmoney24 transfer c2c another bank	5.00	
 Send Money 24 Ltd	0.01	

How to lose money during payment research



How to lose money during payment research

https://medium.com/@Tim_Y/how-to-lose-money-during-payment-research-or-in-searching-for-financial-ombudsman-5047bff89bc2





Who will pay?

- Not all vendors/banks are the same
- Risk-based model doesn't care "where's the money", but "how much money"

Bugbounty company from Google

1. Found vulnerability
2. Reported with lowest CVSS/out of scope
3. Thanks, \$\$\$
4. Now vulnerabilities won't be used in the wild

Bank "A"

1. Found vulnerability
2. Reported medium CVSS
3. It's not been used in the wild
4. Vulnerabilities still can be used in the wild



<https://www.cardpayments.fail>



info (at) cardpayments (dot) fail



@a66ot