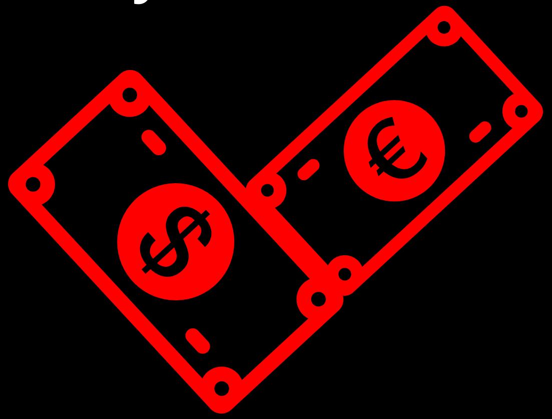
FOR THE LOVE OF MONEY

Finding and exploiting vulnerabilities in mobile point of sales systems



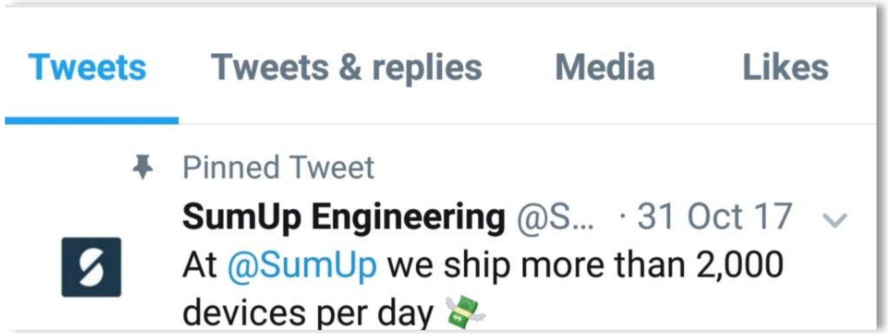
LEIGH-ANNE GALLOWAY & TIM YUNUSOV

POSITIVE TECHNOLOGIES

MPOS GROWTH

2010

Single vendor



Pinned Tweet

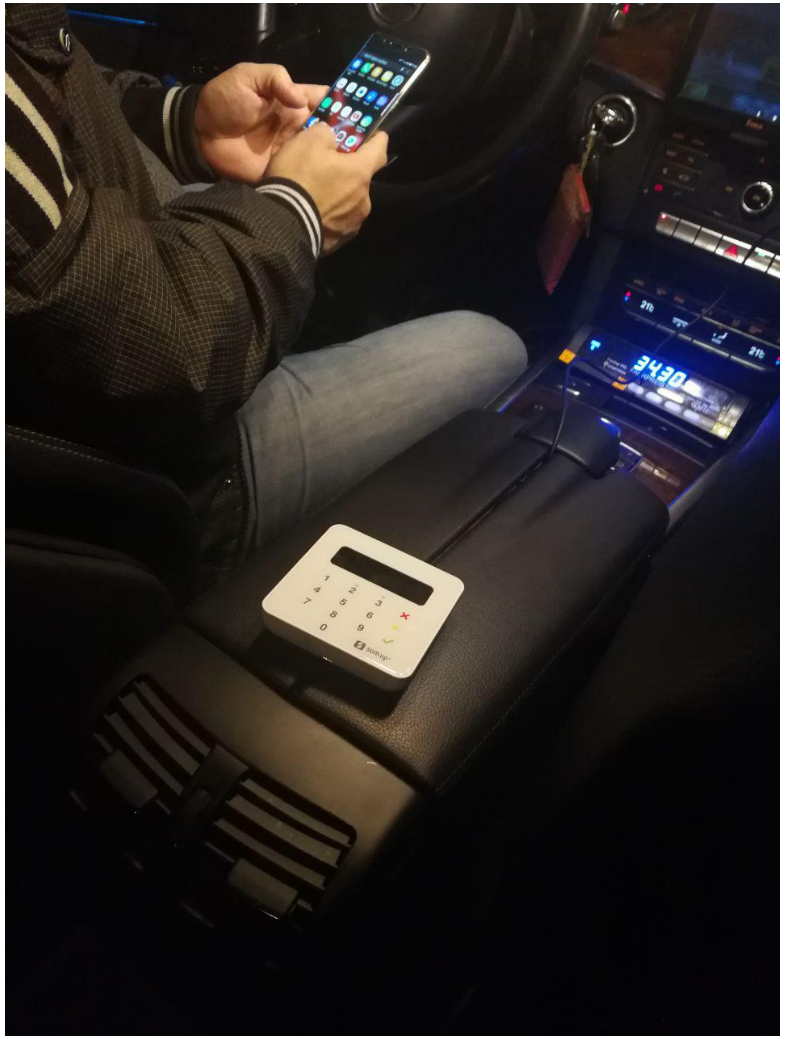
SumUp Engineering @S... · 31 Oct 17

At @SumUp we ship more than 2,000 devices per day 💸

2018

Four leading vendors
shipping thousands of units per day

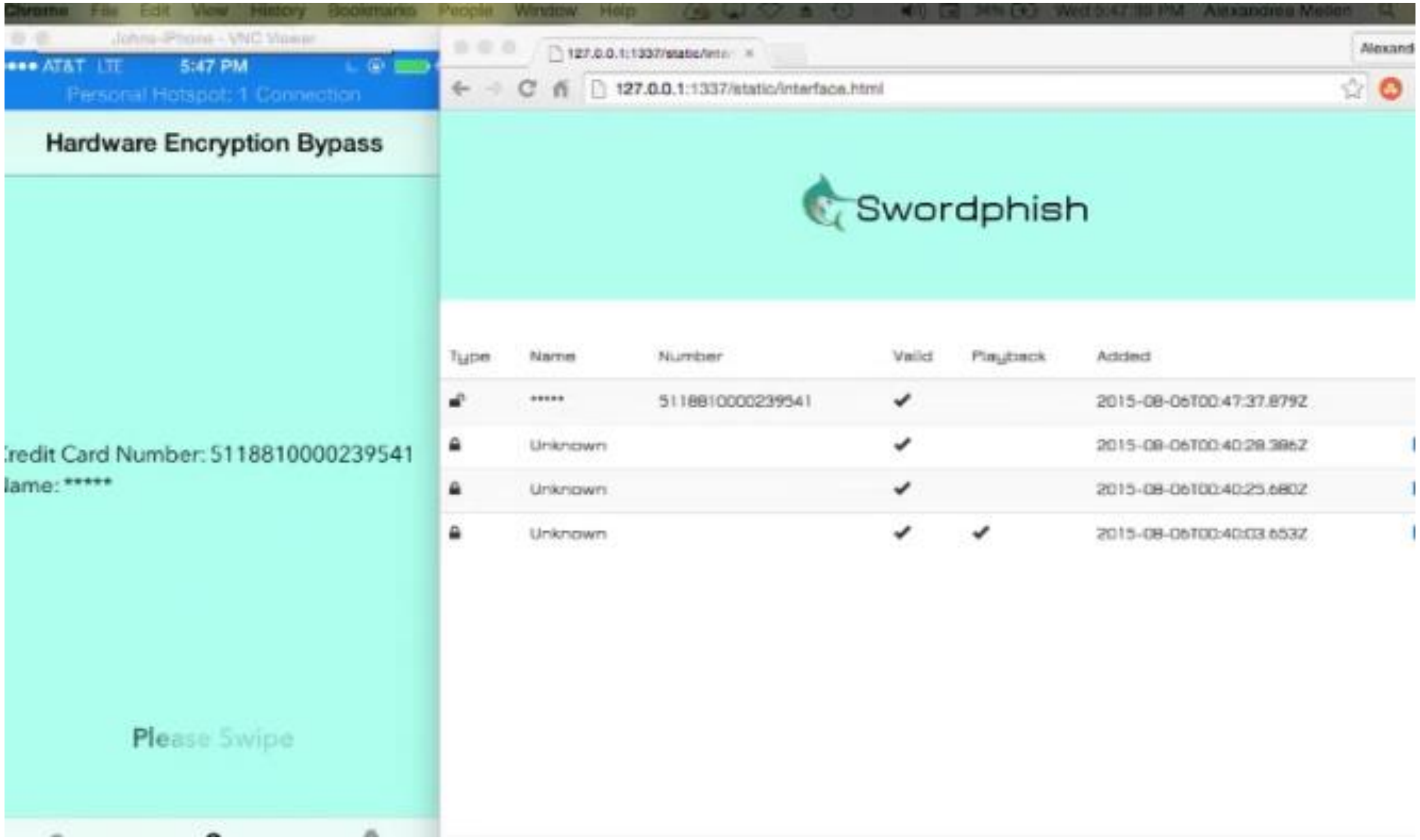
Motivations



Related Work

MWR Labs “Mission mPOSsible” 2014

Related Work

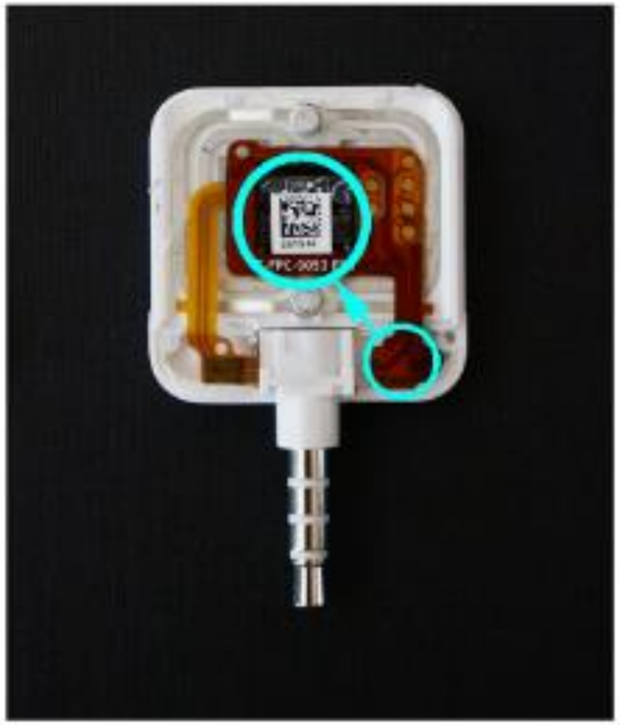

Chrome File Edit View History Bookmarks People Window Help
Johns-iPhone - VNC Viewer
AT&T LTE 5:47 PM
Personal Hotspot: 1 Connection
127.0.0.1:1337/static/interface.html
Swordphish

Hardware Encryption Bypass

redit Card Number: 5118810000239541
lame: *****

Please Swipe

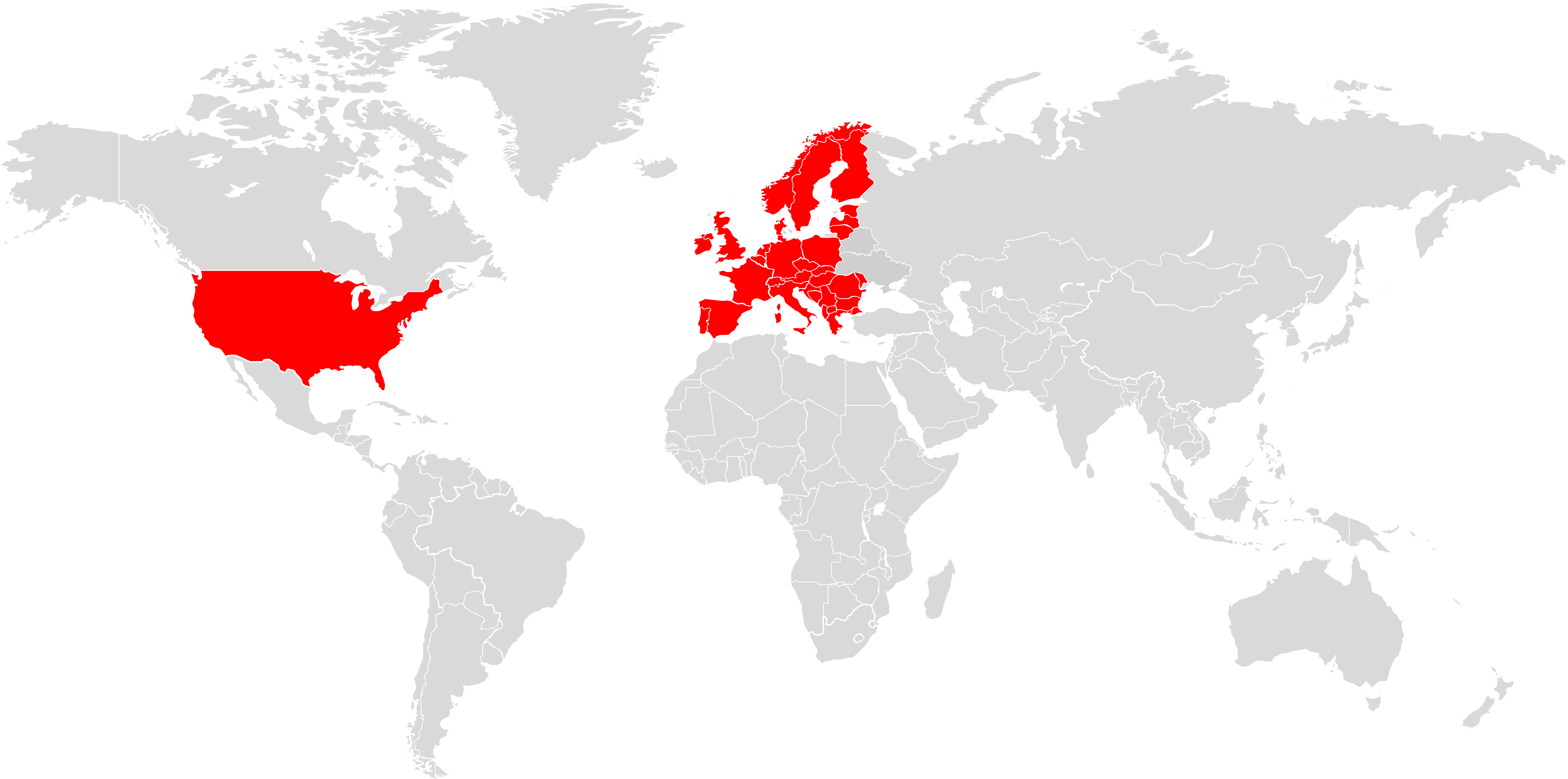
Type	Name	Number	Valid	Playback	Added
🔓	*****	5118810000239541	✓		2015-08-06T00:47:37.879Z
🔒	Unknown		✓		2015-08-06T00:40:28.386Z
🔒	Unknown		✓		2015-08-06T00:40:25.680Z
🔒	Unknown		✓	✓	2015-08-06T00:40:03.653Z



Mellen, Moore and Losev “Mobile Point of Scam: Attacking the Square Reader” (2015)

Research Scope

Research Scope



Research Scope

PAYPAL

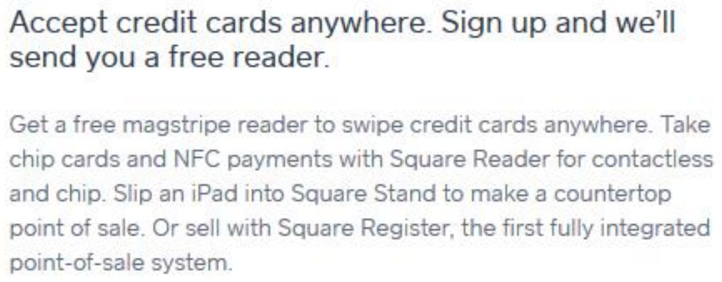
SQUARE

IZETTLE

SUMUP

Research Scope

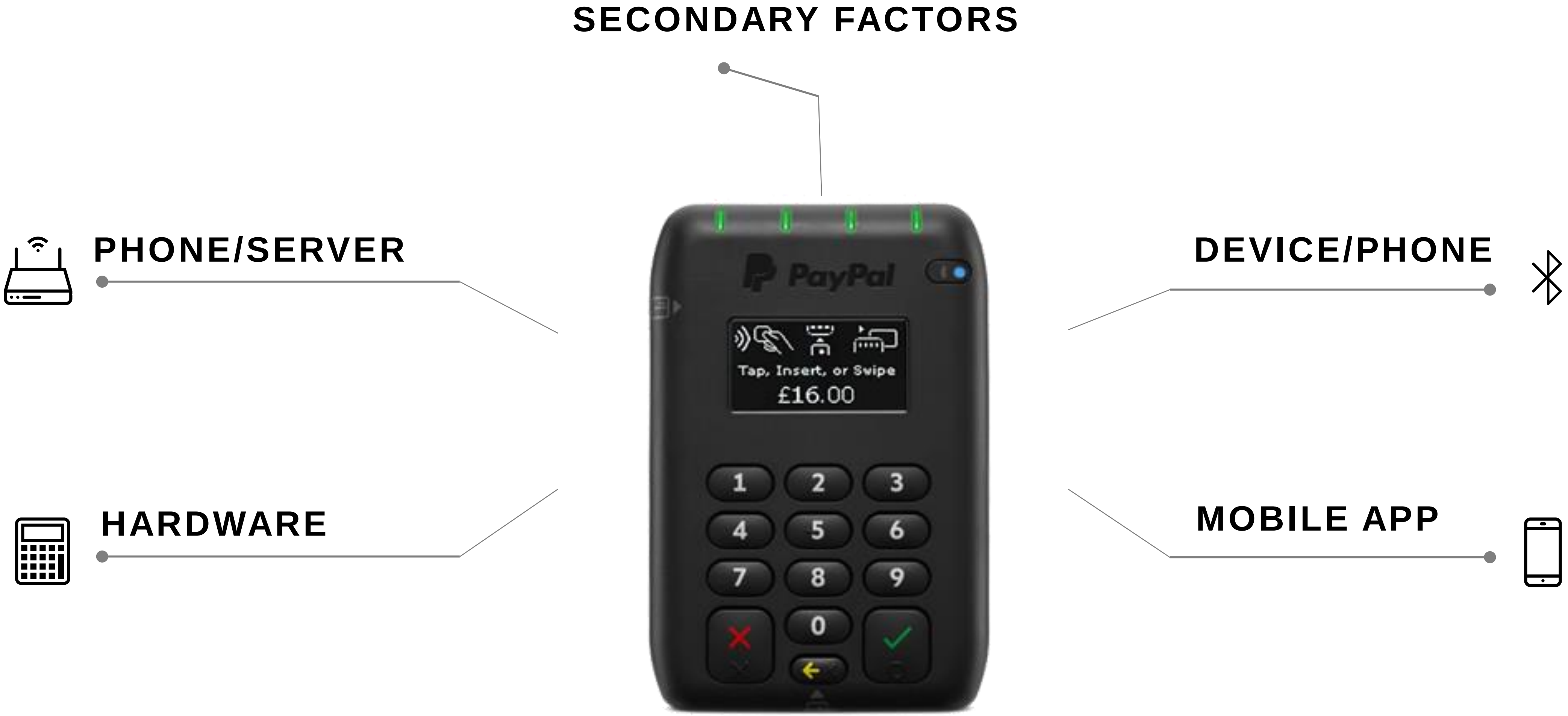
“How much security can really be embedded in a device that is free?”



Accept credit cards anywhere. Sign up and we’ll send you a free reader.

Get a free magstripe reader to swipe credit cards anywhere. Take chip cards and NFC payments with Square Reader for contactless and chip. Slip an iPad into Square Stand to make a countertop point of sale. Or sell with Square Register, the first fully integrated point-of-sale system.

Research Scope



SECONDARY FACTORS

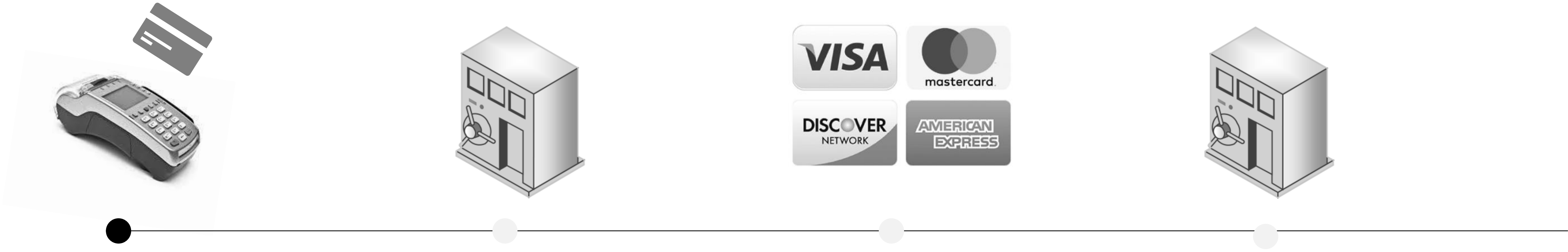
PHONE/SERVER

DEVICE/PHONE

HARDWARE

MOBILE APP

Background



MERCHANT

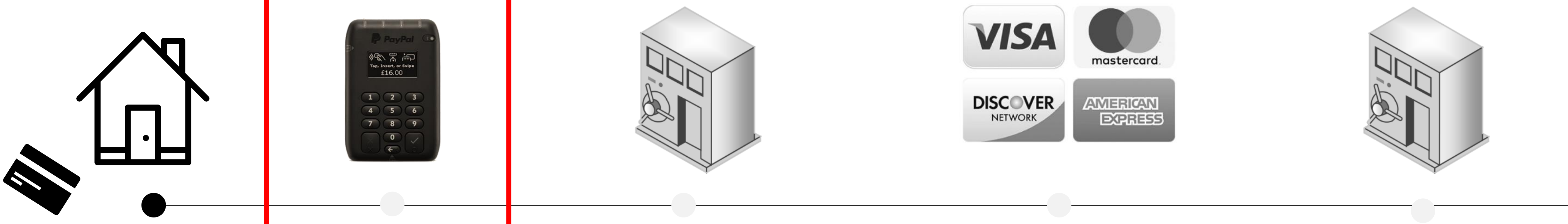
ACQUIRER

CARD BRANDS

ISSUER

Background

MERCHANT



MERCHANT

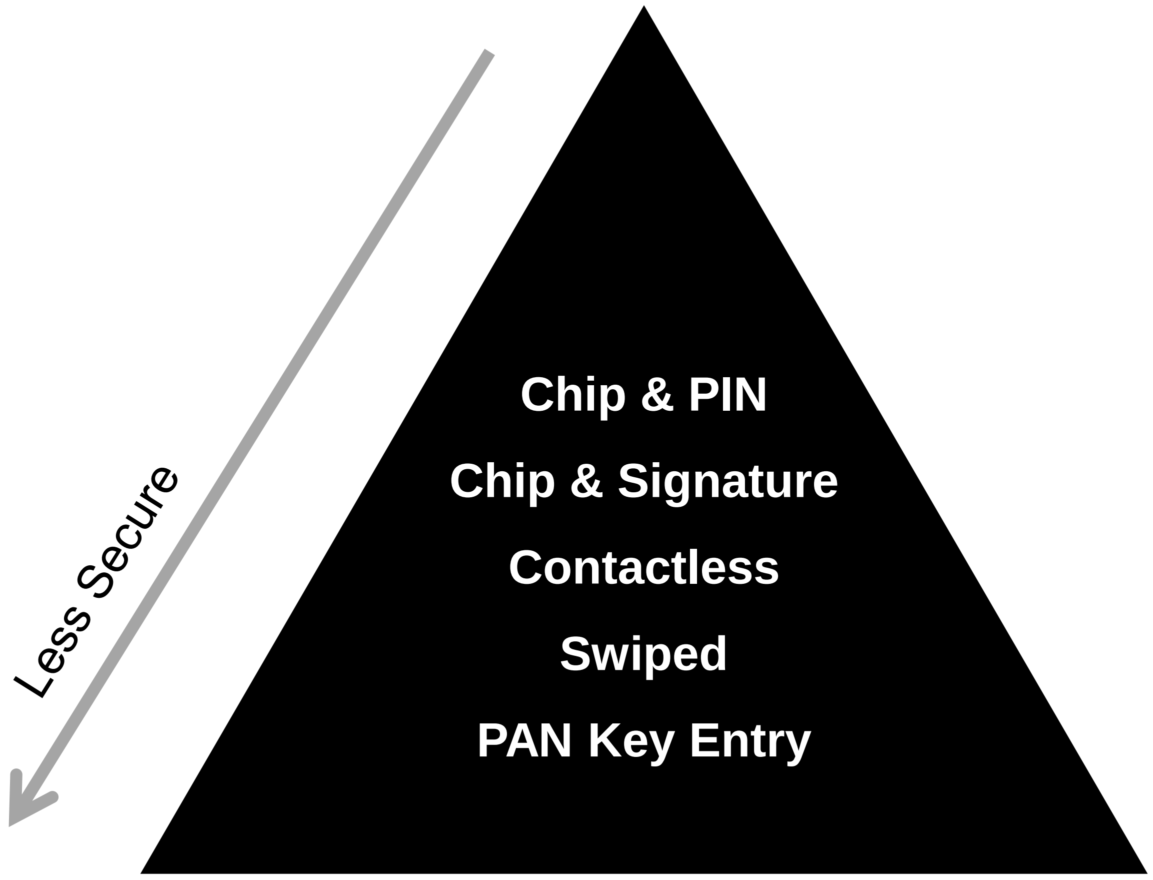
MPOS PROVIDER

ACQUIRER

CARD BRANDS

ISSUER

CARD RISK BY OPERATION TYPE



Chip & PIN

Chip & Signature

Contactless

Swiped

PAN Key Entry

GLOBAL ADOPTION OF EMV - POS TERMINALS

EU EMV ACCEPTANCE

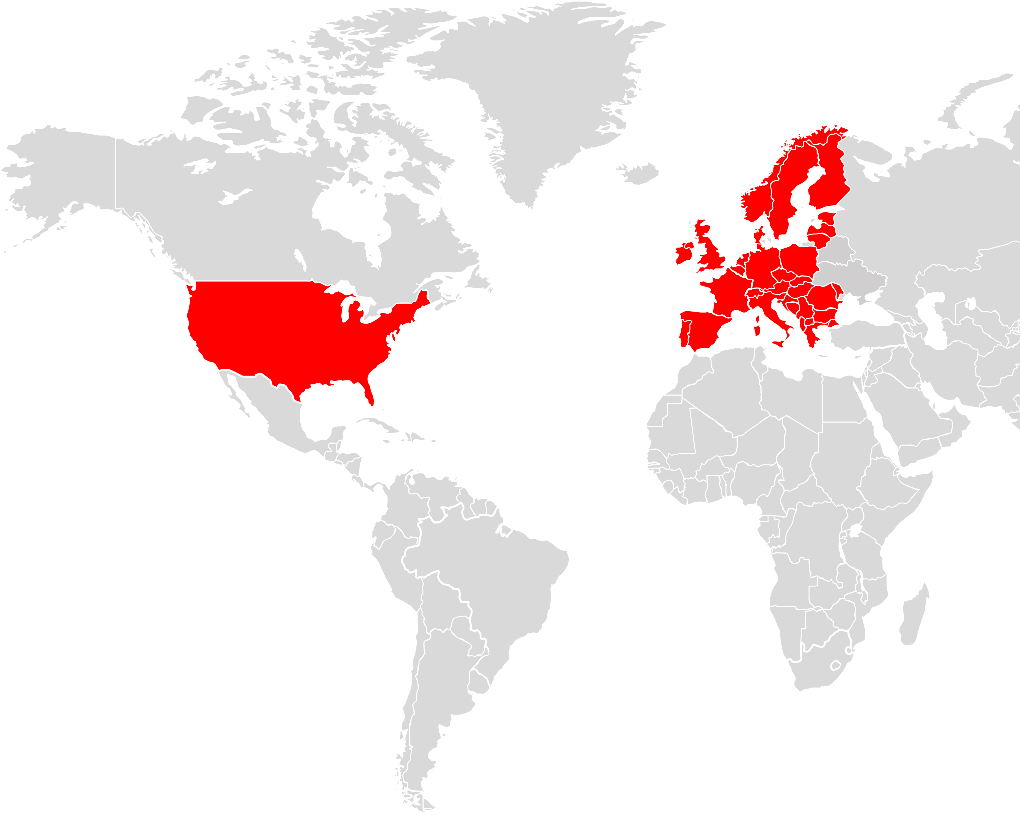
EMV enabled POS devices make up between 90-95% of POS population

90%

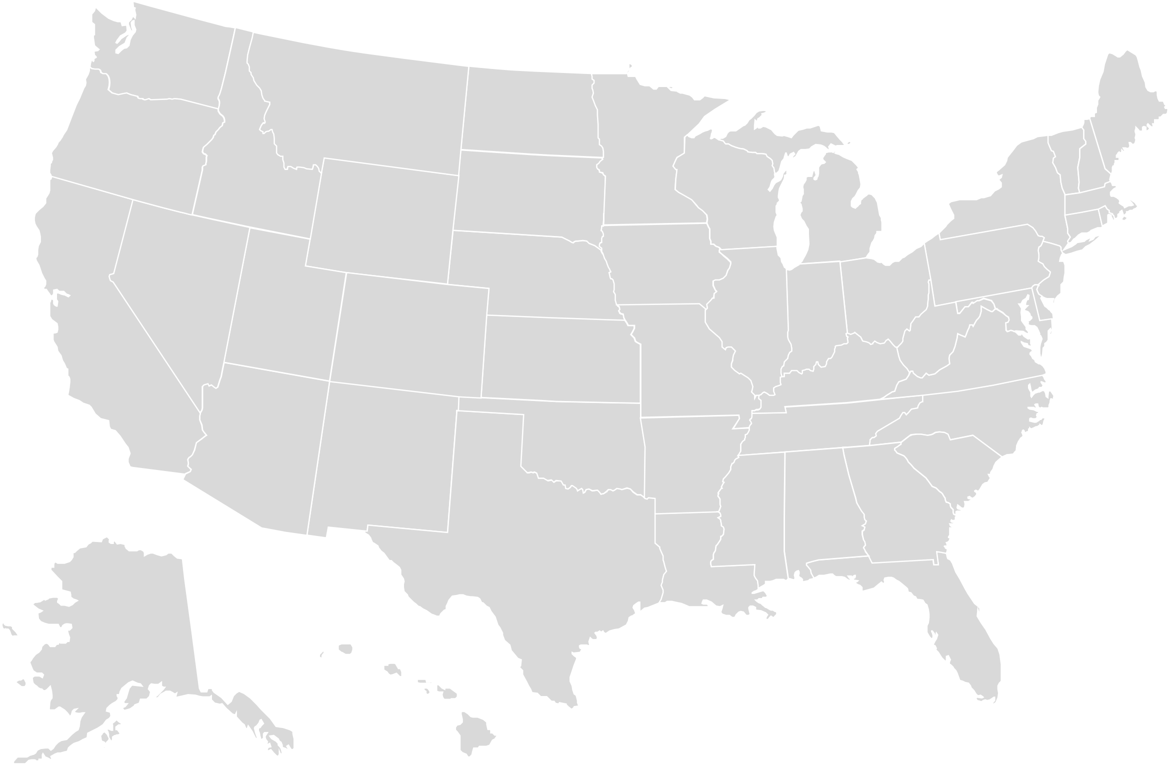
US EMV ACCEPTANCE

EMV enabled POS devices make up 13% of POS population and 9% of the ATM population

13%



Background



EMV CREDIT CARD ADOPTION

96% of credit cards in circulation support EMV as a protocol

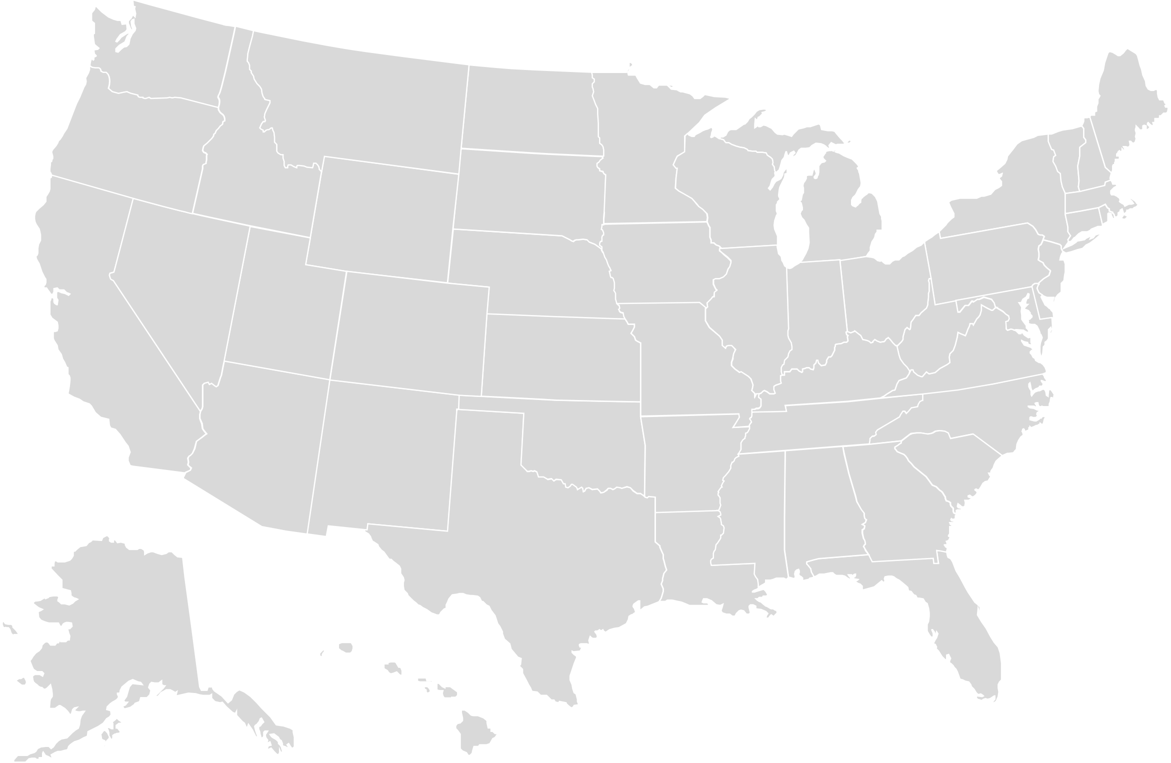
96%

EMV CREDIT CARD USAGE

However less than half of all transactions are made by chip

41%

Background



EMV DEBIT CARD ADOPTION

79% of debit cards in circulation support EMV as a protocol

79%

EMV DEBIT CARD USAGE

However less than half of all transactions are made using chip

23%

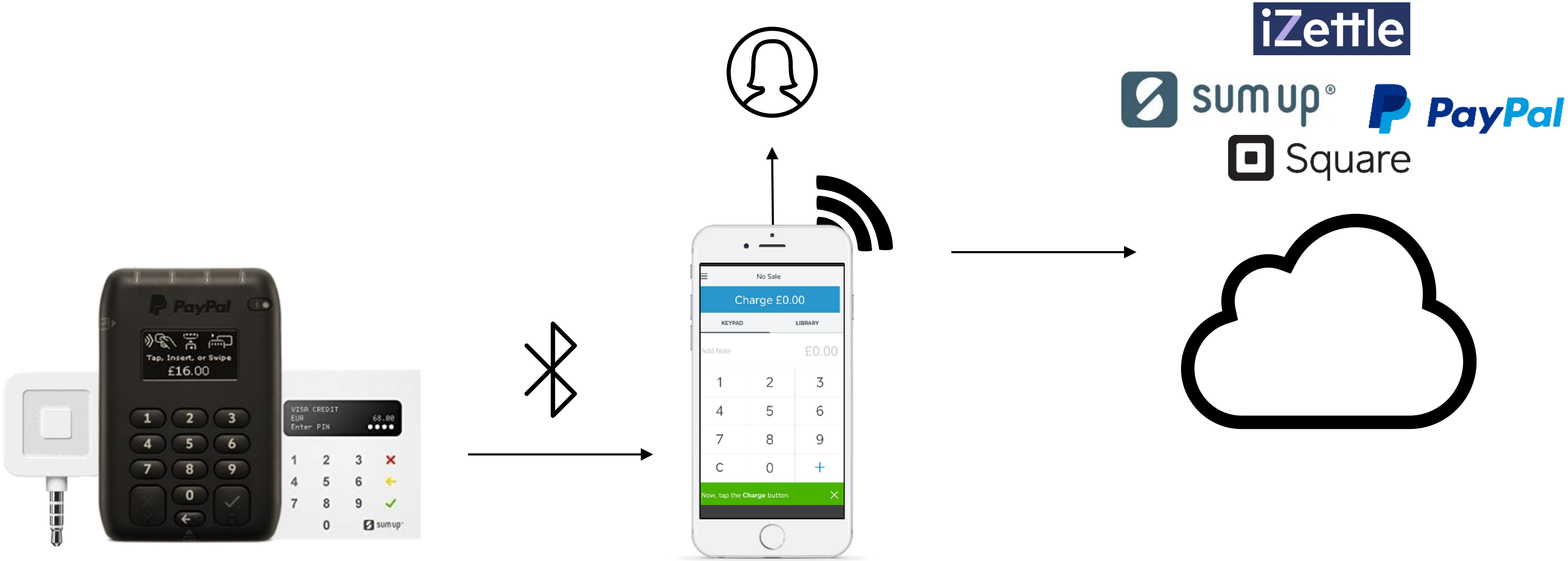
Background

MPOS TIMELINE 2019

PERCENTAGE OF TRANSACTIONS — 46%

52 — MILLIONS OF NUMBER OF UNITS

SCHEMATIC OVERVIEW OF COMPONENTS

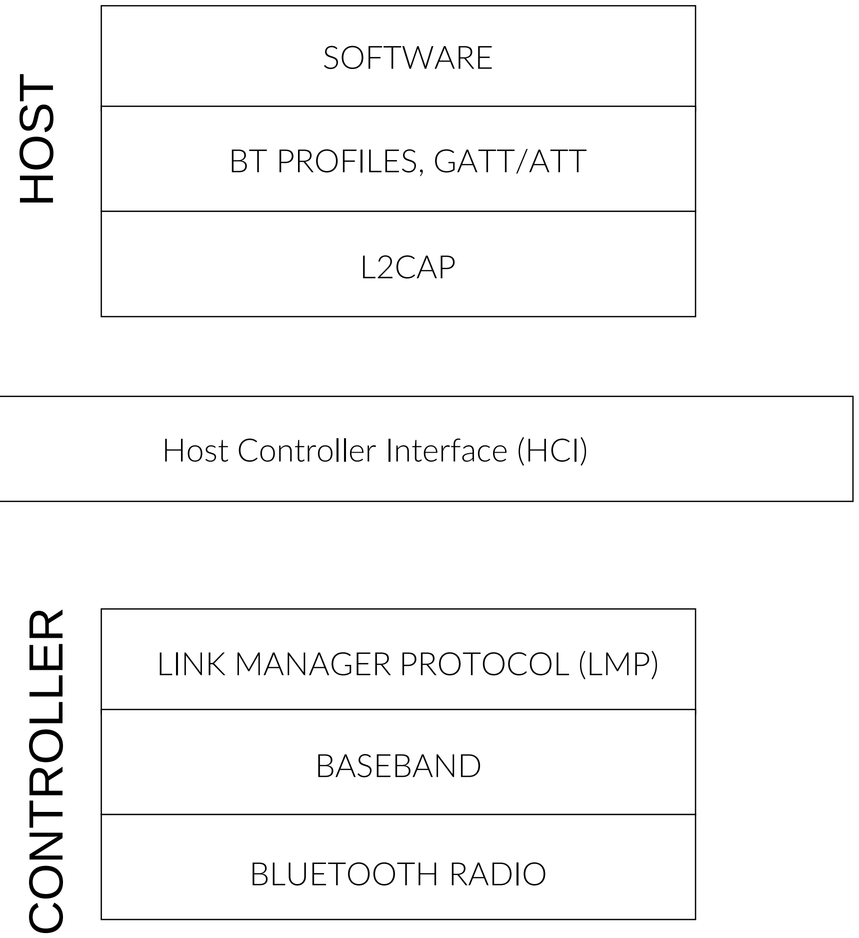


FINDINGS

- SENDING ARBITRARY COMMANDS
- AMOUNT MODIFICATION
- REMOTE CODE EXECUTION
- HARDWARE OBSERVATIONS
- SECONDARY FACTORS

BLUETOOTH

BLUETOOTH PROTOCOL



HOST

SOFTWARE

BT PROFILES, GATT/ATT

L2CAP

Host Controller Interface (HCI)

CONTROLLER

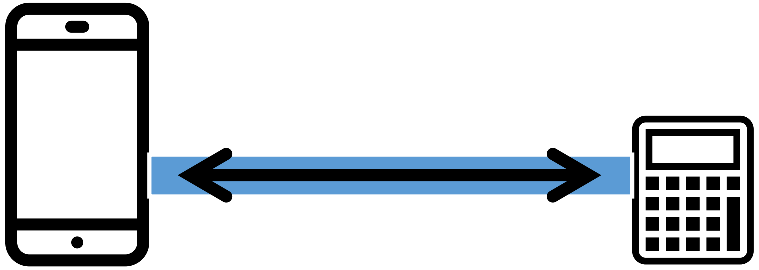
LINK MANAGER PROTOCOL (LMP)

BASEBAND

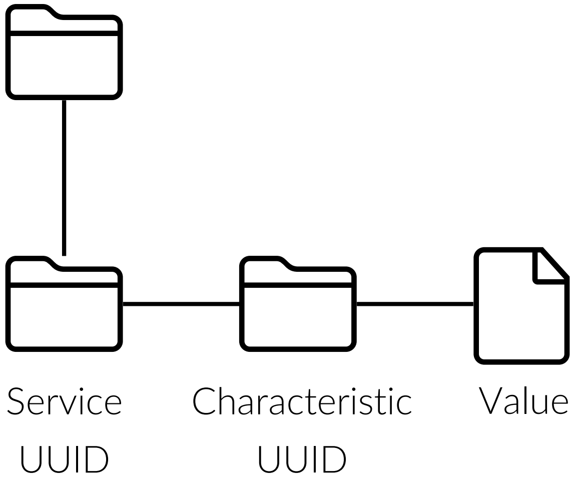
BLUETOOTH RADIO

Methods & Tools

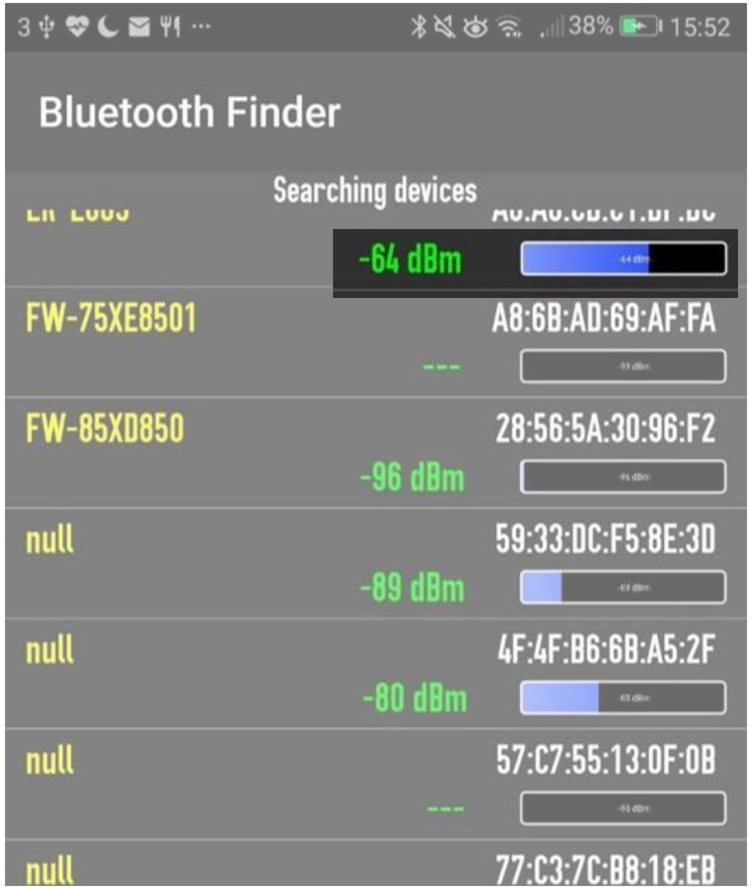
RFCOMM



GATT (Generic Attribute) /ATT(Attribute Protocol)



BLUETOOTH AS A COMMUNICATION CHANNEL



3 38% 15:52

Bluetooth Finder

Searching devices

-64 dBm

FW-75XE8501 A8:6B:AD:69:AF:FA

FW-85XD850 28:56:5A:30:96:F2
-96 dBm

null 59:33:DC:F5:8E:3D
-89 dBm

null 4F:4F:B6:6B:A5:2F
-80 dBm

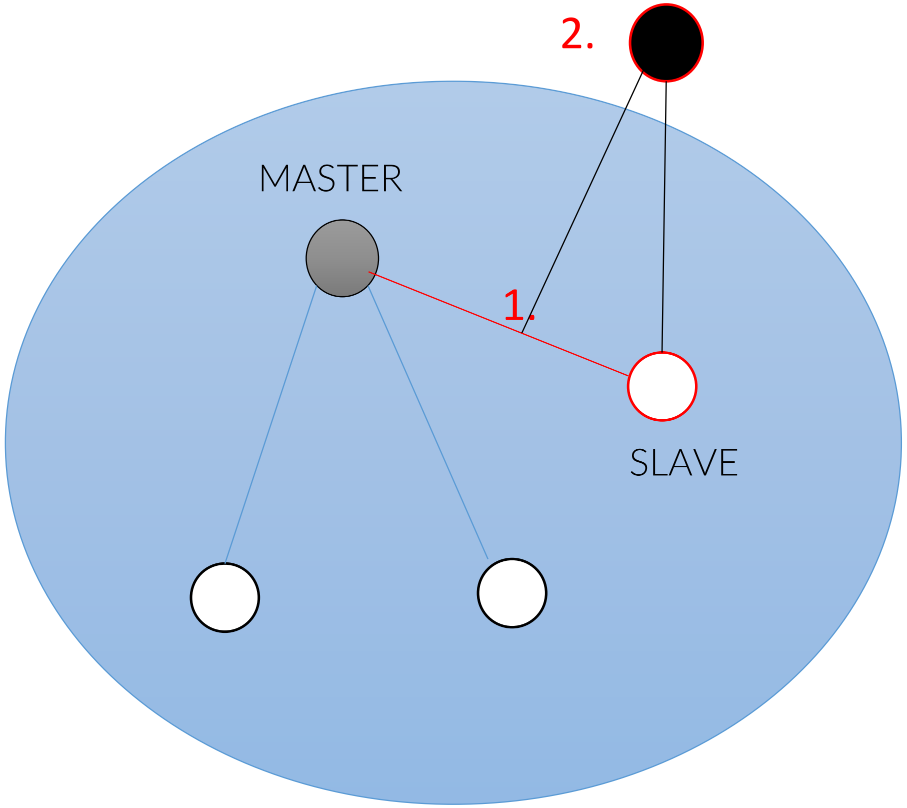
null 57:C7:55:13:0F:0B
---

null 77:C3:7C:B8:18:EB

NAP	UAP	LAP
68:AA	D2	0D:CC:3E
Org Unique Identifier		Unique to device

BLUETOOTH ATTACK VECTORS

- Eavesdropping/MITM
- Manipulating characteristics



Methods & Tools

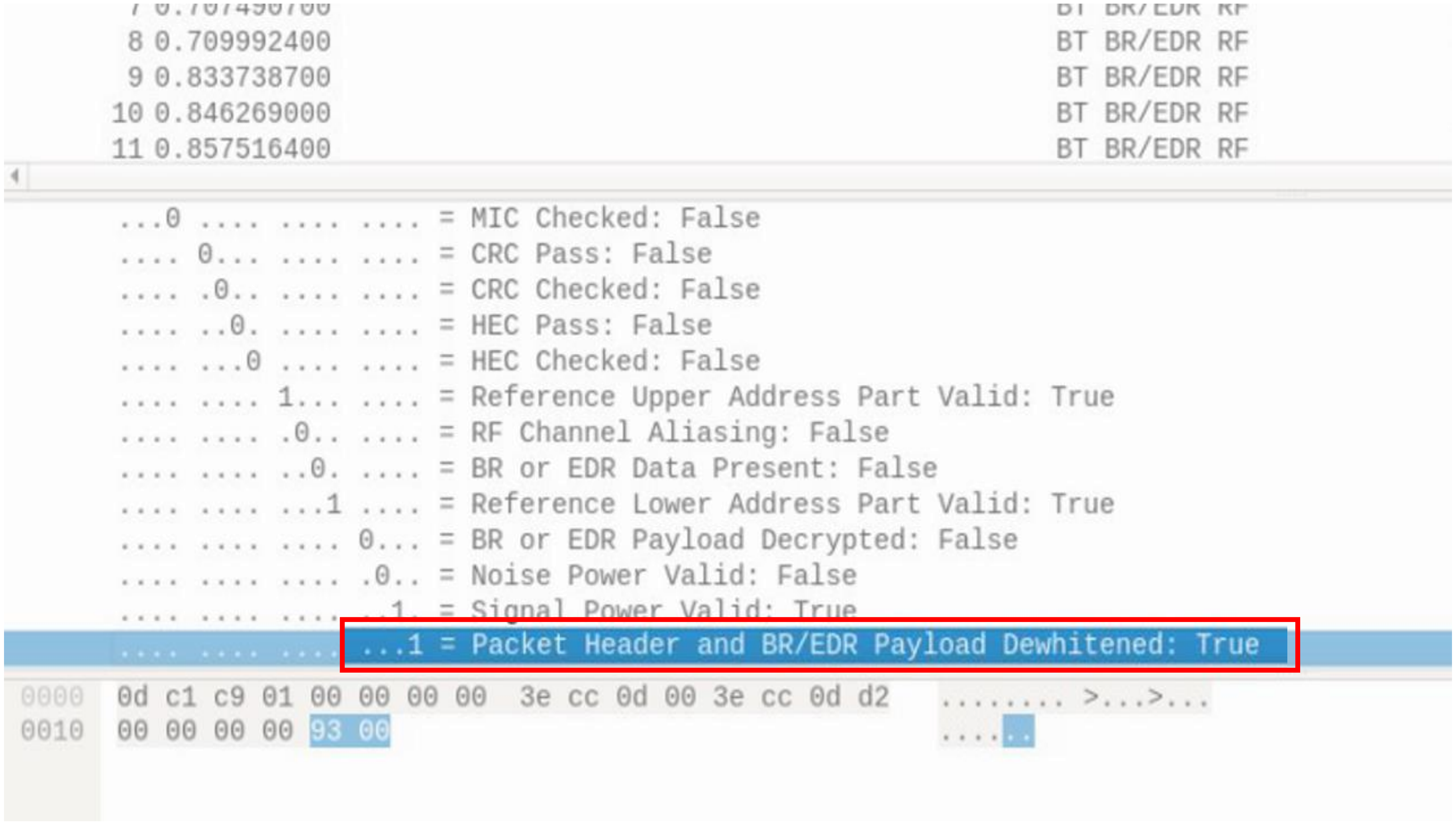
Frontline BPA 600

$20,000

Ubertooth One

$120

Methods & Tools

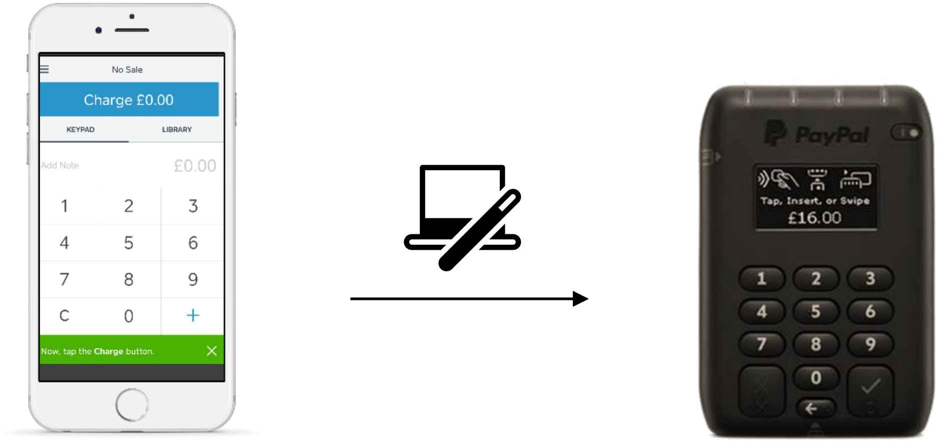


```
 7 0.707490700                                                BT BR/EDR RF
 8 0.709992400                                                BT BR/EDR RF
 9 0.833738700                                                BT BR/EDR RF
10 0.846269000                                                BT BR/EDR RF
11 0.857516400                                                BT BR/EDR RF

...0 .... .... .... = MIC Checked: False
.... 0... .... .... = CRC Pass: False
.... .0.. .... .... = CRC Checked: False
.... ..0. .... .... = HEC Pass: False
.... ...0 .... .... = HEC Checked: False
.... .... 1... .... = Reference Upper Address Part Valid: True
.... .... .0.. .... = RF Channel Aliasing: False
.... .... ..0. .... = BR or EDR Data Present: False
.... .... ...1 .... = Reference Lower Address Part Valid: True
.... .... .... 0... = BR or EDR Payload Decrypted: False
.... .... .... .0.. = Noise Power Valid: False
.... .... .... ..1. = Signal Power Valid: True
.... .... .... ...1 = Packet Header and BR/EDR Payload Dewhitened: True

0000  0d c1 c9 01 00 00 00 00  3e cc 0d 00 3e cc 0d d2   ........ >...>...
0010  00 00 00 00 93 00                                  ......
```

SENDING ARBITRARY COMMANDS

MANIPULATING CHARACTERISTICS

- Initiate a function
- Display text
- Turn off or on

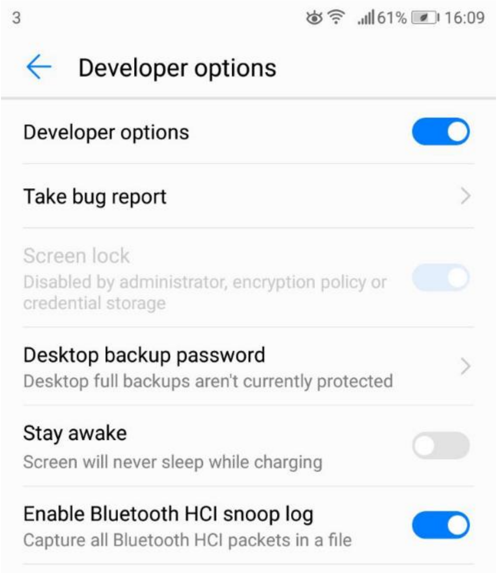


User authentication doesn’t exist in the Bluetooth protocol, it must be added by the developer at the application layer

Findings

1.

2.



3 · 61% · 16:09

← Developer options

Developer options ●

Take bug report ›

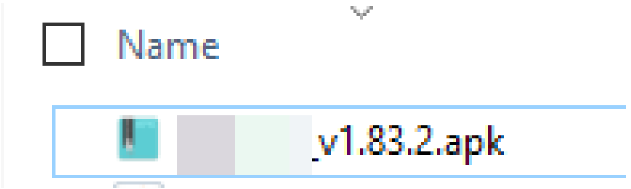
Screen lock
Disabled by administrator, encryption policy or credential storage

Desktop backup password ›
Desktop full backups aren't currently protected

Stay awake ○
Screen will never sleep while charging

Enable Bluetooth HCI snoop log ●
Capture all Bluetooth HCI packets in a file

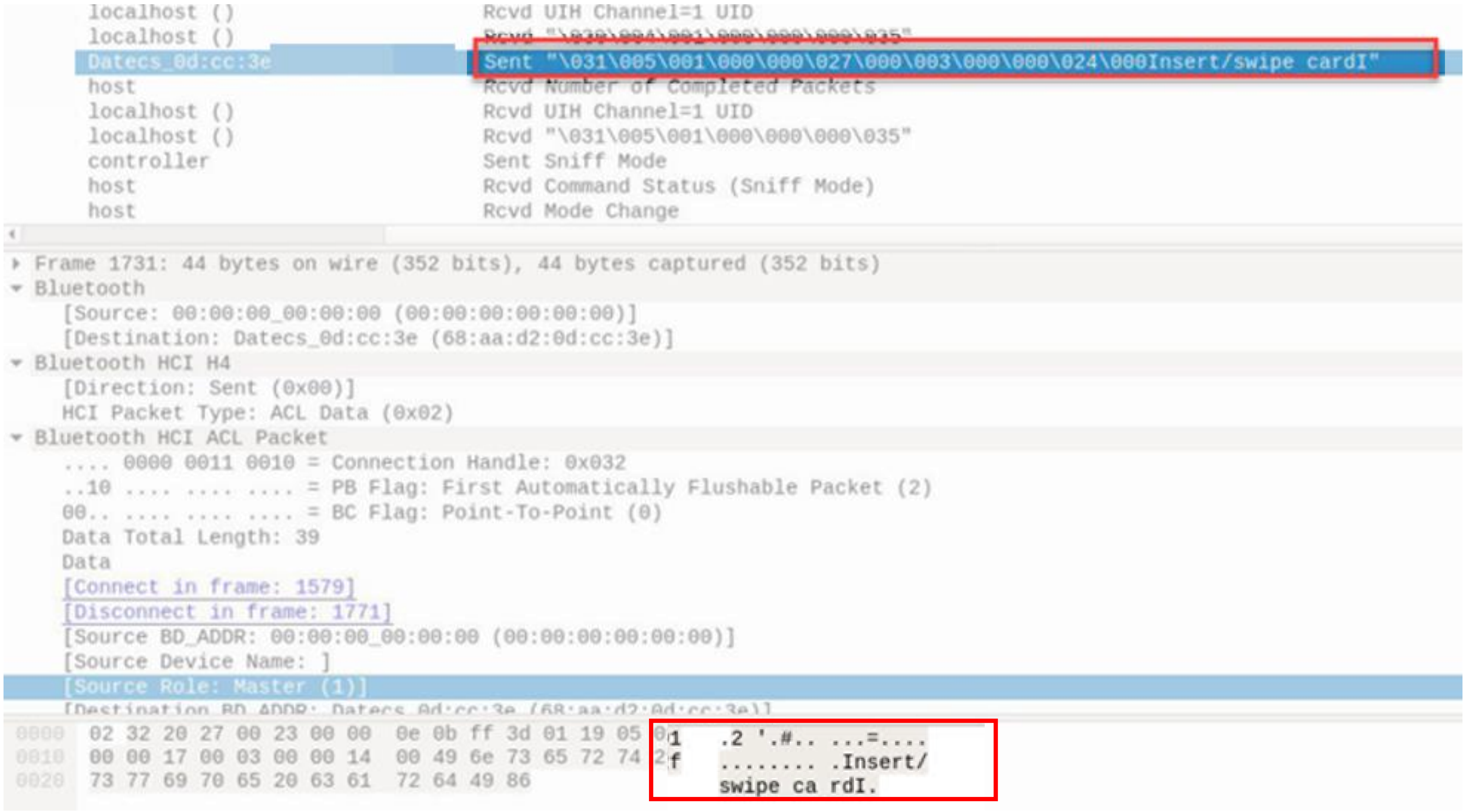
3.



□ Name

[redacted]_v1.83.2.apk

Findings

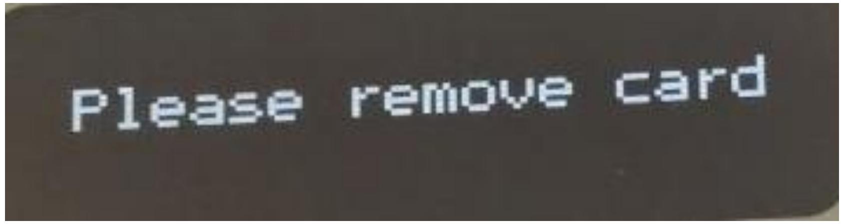


```
localhost ()          Rcvd UIH Channel=1 UID
localhost ()          Rcvd "\030\004\001\000\000\000\035"
Datecs_0d:cc:3e       Sent "\031\005\001\000\000\027\000\003\000\000\024\000Insert/swipe cardI"
host                  Rcvd Number of Completed Packets
localhost ()          Rcvd UIH Channel=1 UID
localhost ()          Rcvd "\031\005\001\000\000\000\035"
controller            Sent Sniff Mode
host                  Rcvd Command Status (Sniff Mode)
host                  Rcvd Mode Change
```

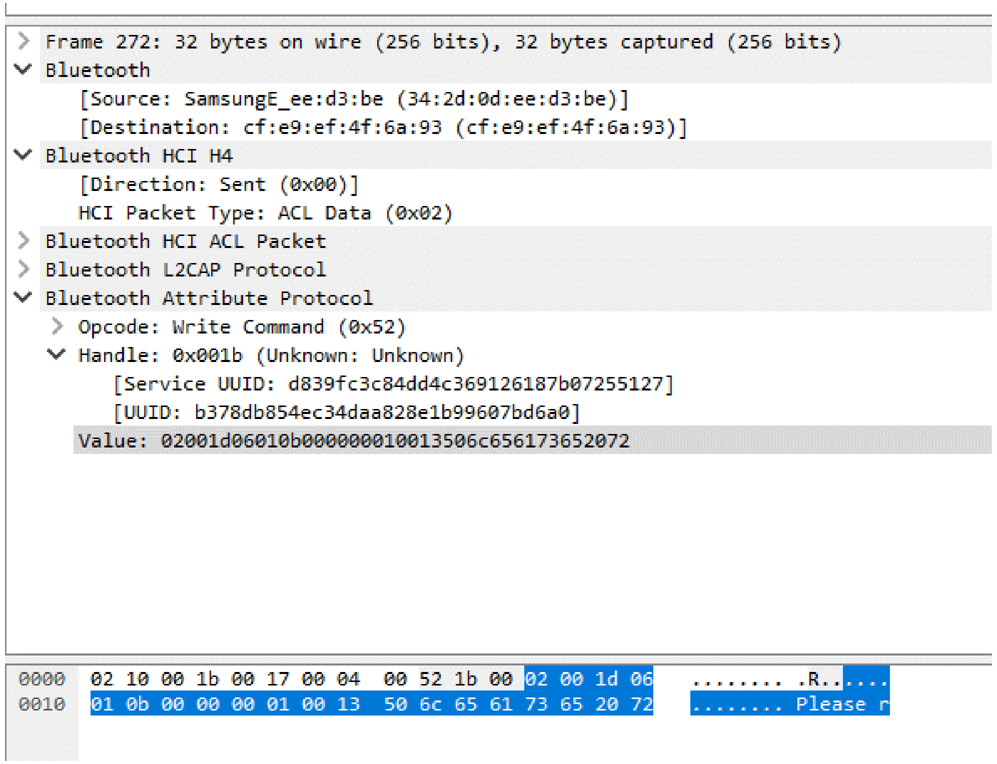
```
▸ Frame 1731: 44 bytes on wire (352 bits), 44 bytes captured (352 bits)
▾ Bluetooth
    [Source: 00:00:00_00:00:00 (00:00:00:00:00:00)]
    [Destination: Datecs_0d:cc:3e (68:aa:d2:0d:cc:3e)]
▾ Bluetooth HCI H4
    [Direction: Sent (0x00)]
    HCI Packet Type: ACL Data (0x02)
▾ Bluetooth HCI ACL Packet
    .... 0000 0011 0010 = Connection Handle: 0x032
    ..10 .... .... .... = PB Flag: First Automatically Flushable Packet (2)
    00.. .... .... .... = BC Flag: Point-To-Point (0)
    Data Total Length: 39
    Data
    [Connect in frame: 1579]
    [Disconnect in frame: 1771]
    [Source BD_ADDR: 00:00:00_00:00:00 (00:00:00:00:00:00)]
    [Source Device Name: ]
    [Source Role: Master (1)]
    [Destination BD_ADDR: Datecs_0d:cc:3e (68:aa:d2:0d:cc:3e)]
```

```
0000  02 32 20 27 00 23 00 00  0e 0b ff 3d 01 19 05 01     .2 '.#.. ...=....
0010  00 00 17 00 03 00 00 14  00 49 6e 73 65 72 74 2f     ........ .Insert/
0020  73 77 69 70 65 20 63 61  72 64 49 86                 swipe ca rdI.
```

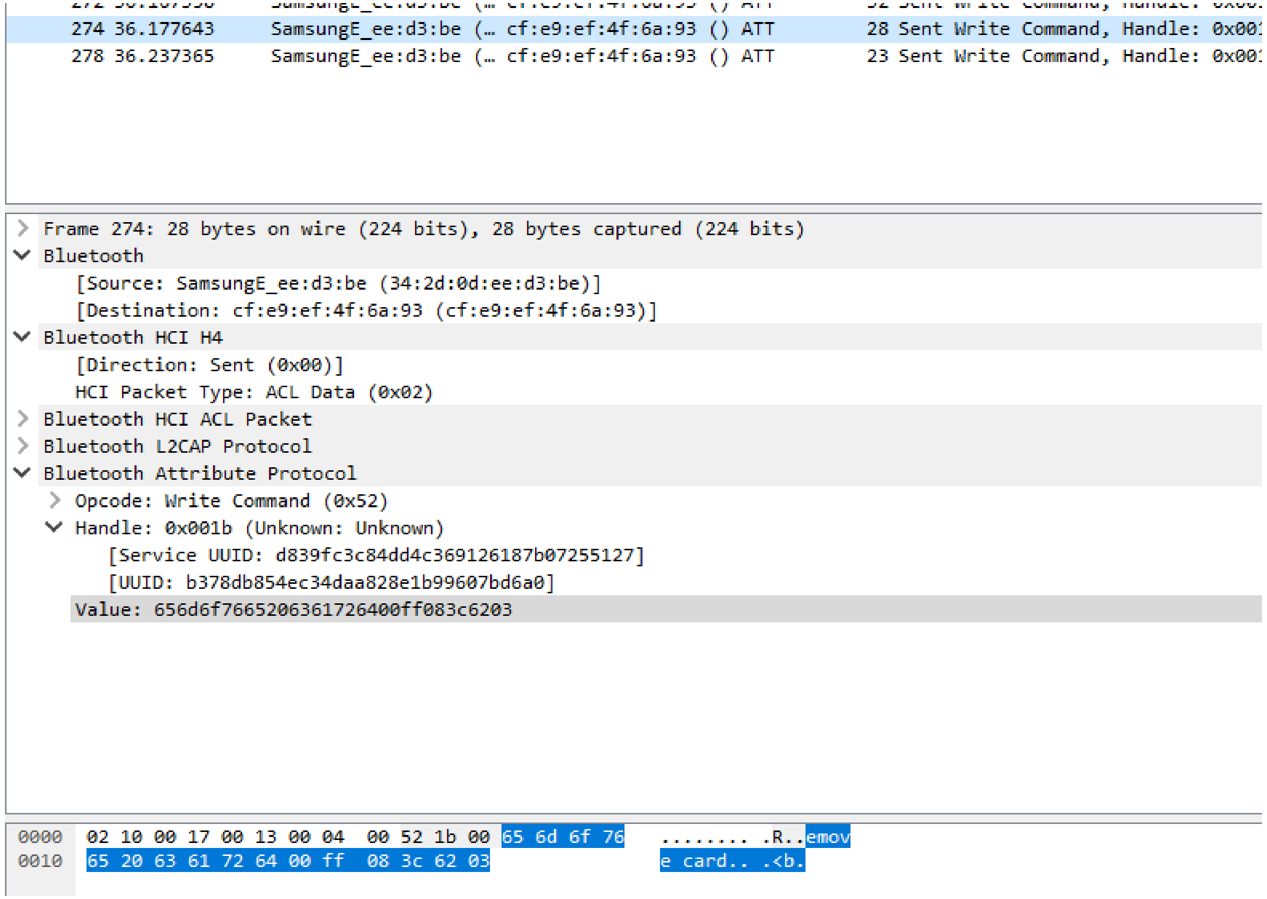
Findings



Please remove card

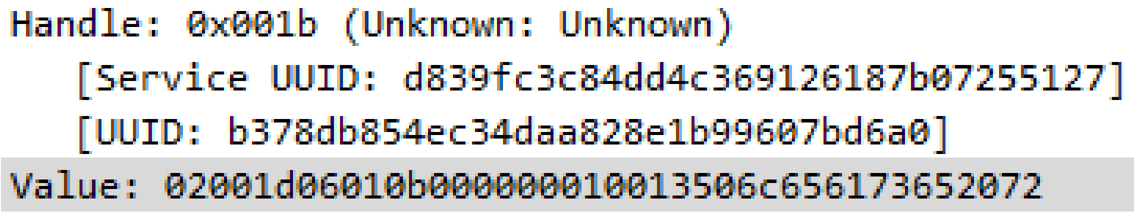


```
> Frame 272: 32 bytes on wire (256 bits), 32 bytes captured (256 bits)
v Bluetooth
    [Source: SamsungE_ee:d3:be (34:2d:0d:ee:d3:be)]
    [Destination: cf:e9:ef:4f:6a:93 (cf:e9:ef:4f:6a:93)]
v Bluetooth HCI H4
    [Direction: Sent (0x00)]
    HCI Packet Type: ACL Data (0x02)
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth Attribute Protocol
  > Opcode: Write Command (0x52)
  v Handle: 0x001b (Unknown: Unknown)
      [Service UUID: d839fc3c84dd4c369126187b07255127]
      [UUID: b378db854ec34daa828e1b99607bd6a0]
    Value: 02001d06010b000000010013506c656173652072

0000  02 10 00 1b 00 17 00 04  00 52 1b 00 02 00 1d 06   ........ .R......
0010  01 0b 00 00 00 01 00 13  50 6c 65 61 73 65 20 72   ........ Please r
```

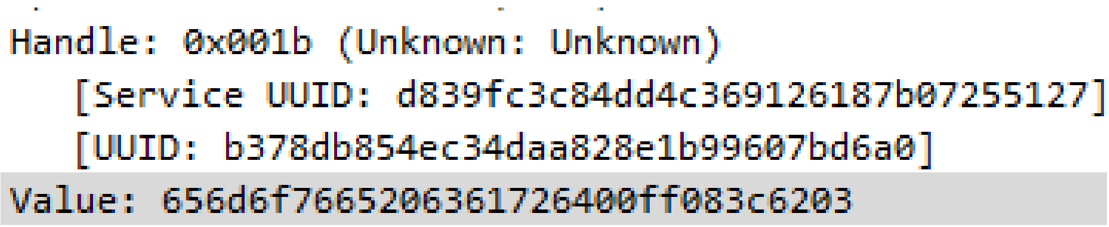


```
274 36.177643   SamsungE_ee:d3:be (… cf:e9:ef:4f:6a:93 () ATT   28 Sent Write Command, Handle: 0x00
278 36.237365   SamsungE_ee:d3:be (… cf:e9:ef:4f:6a:93 () ATT   23 Sent Write Command, Handle: 0x00

> Frame 274: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
v Bluetooth
    [Source: SamsungE_ee:d3:be (34:2d:0d:ee:d3:be)]
    [Destination: cf:e9:ef:4f:6a:93 (cf:e9:ef:4f:6a:93)]
v Bluetooth HCI H4
    [Direction: Sent (0x00)]
    HCI Packet Type: ACL Data (0x02)
> Bluetooth HCI ACL Packet
> Bluetooth L2CAP Protocol
v Bluetooth Attribute Protocol
  > Opcode: Write Command (0x52)
  v Handle: 0x001b (Unknown: Unknown)
      [Service UUID: d839fc3c84dd4c369126187b07255127]
      [UUID: b378db854ec34daa828e1b99607bd6a0]
    Value: 656d6f7665206361726400ff083c6203

0000  02 10 00 17 00 13 00 04  00 52 1b 00 65 6d 6f 76   ........ .R..emov
0010  65 20 63 61 72 64 00 ff  08 3c 62 03               e card.. .<b.
```

Findings



```
Handle: 0x001b (Unknown: Unknown)
   [Service UUID: d839fc3c84dd4c369126187b07255127]
   [UUID: b378db854ec34daa828e1b99607bd6a0]
Value: 02001d06010b000000010013506c656173652072
```



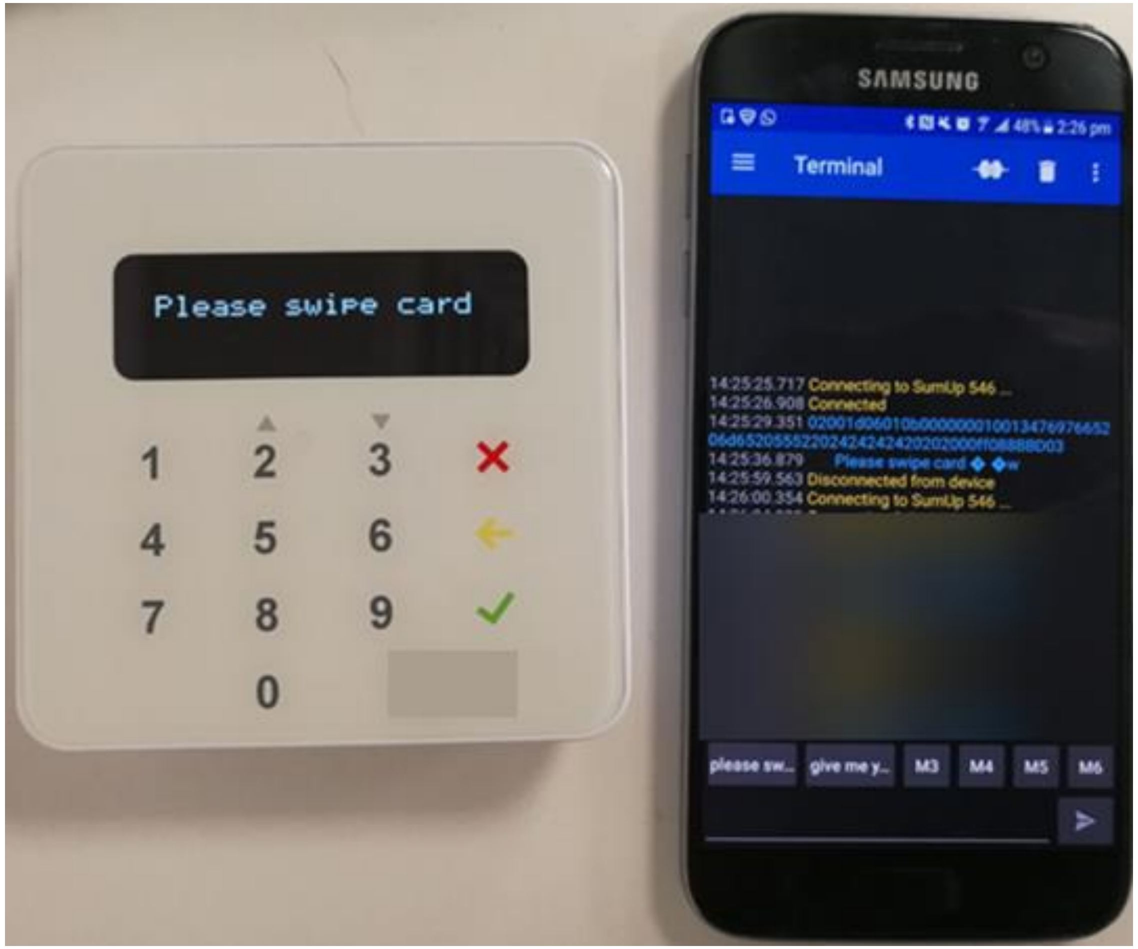
```
Handle: 0x001b (Unknown: Unknown)
   [Service UUID: d839fc3c84dd4c369126187b07255127]
   [UUID: b378db854ec34daa828e1b99607bd6a0]
Value: 656d6f76652063617264 00ff083c6203
```

LEADING PART	MESSAGE	TRAILING PART	CRC	END
02001d06010b000000010013	506c656173652072656d6f76652063617264	00ff08	3c62	03
	“Please remove card”			

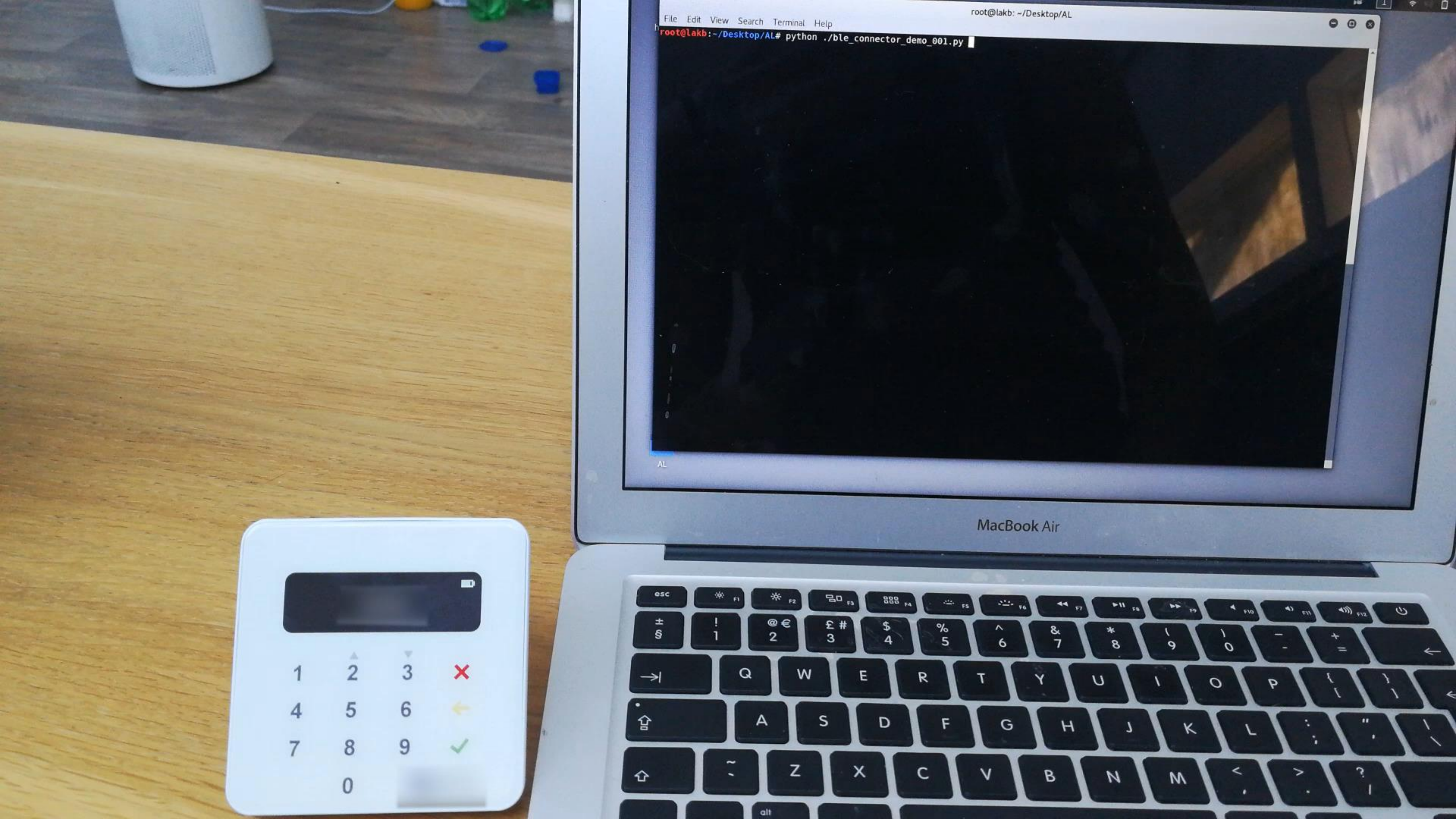
ATTACK VECTORS

1. Force cardholder to use a more vulnerable payment method such as mag-stripe

2. Once the first payment is complete, display “Payment declined”, force cardholder to authorise additional transaction.

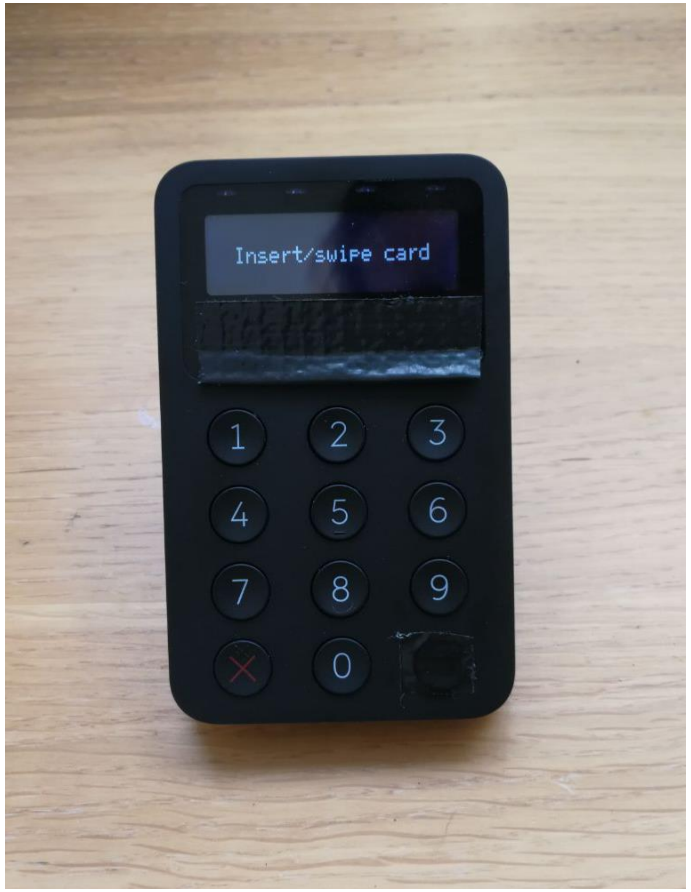


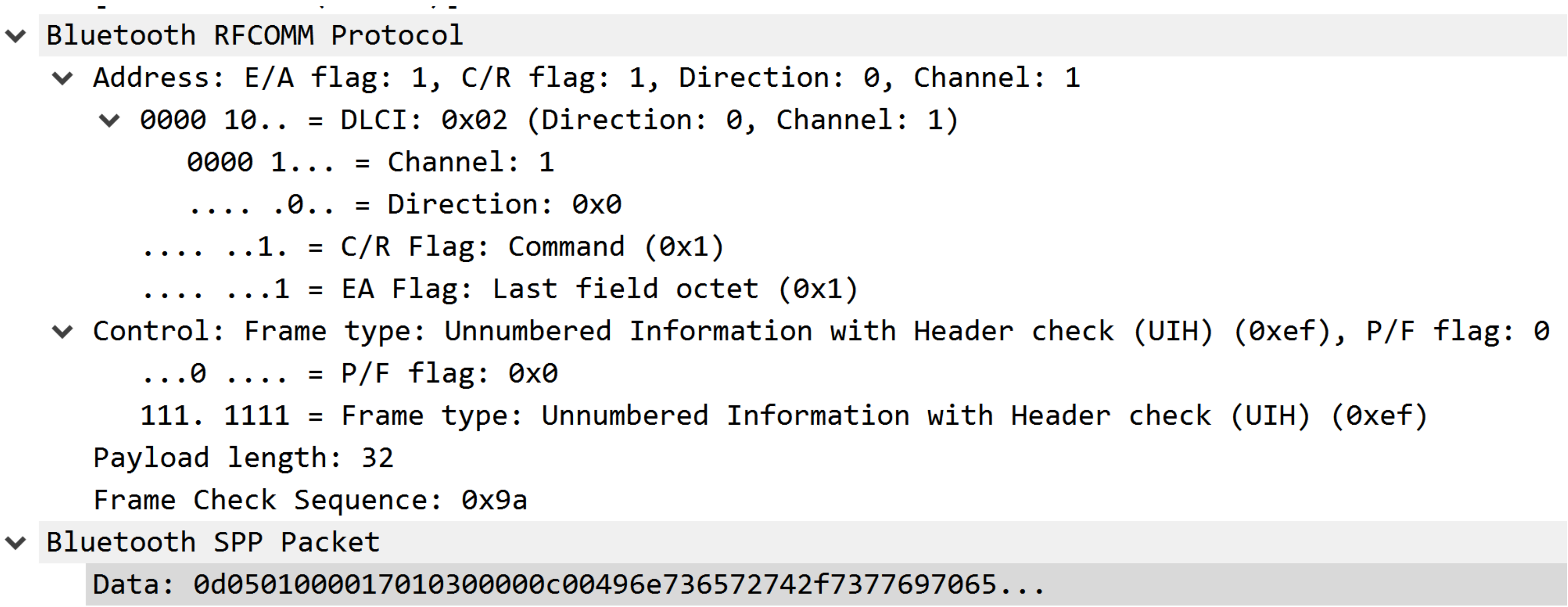
```
14:25:25.717 Connecting to SumUp 546 ...
14:25:26.908 Connected
14:25:29.351 02001d06010b000000001001347697 6652
06d652055522024242424202020000ff08888D03
14:25:36.879      Please swipe card ◆ ◆w
14:25:59.563 Disconnected from device
14:26:00.354 Connecting to SumUp 546 ...
```



```
root@lakb:~/Desktop/AL# python ./ble_connector_demo_001.py
```

Findings

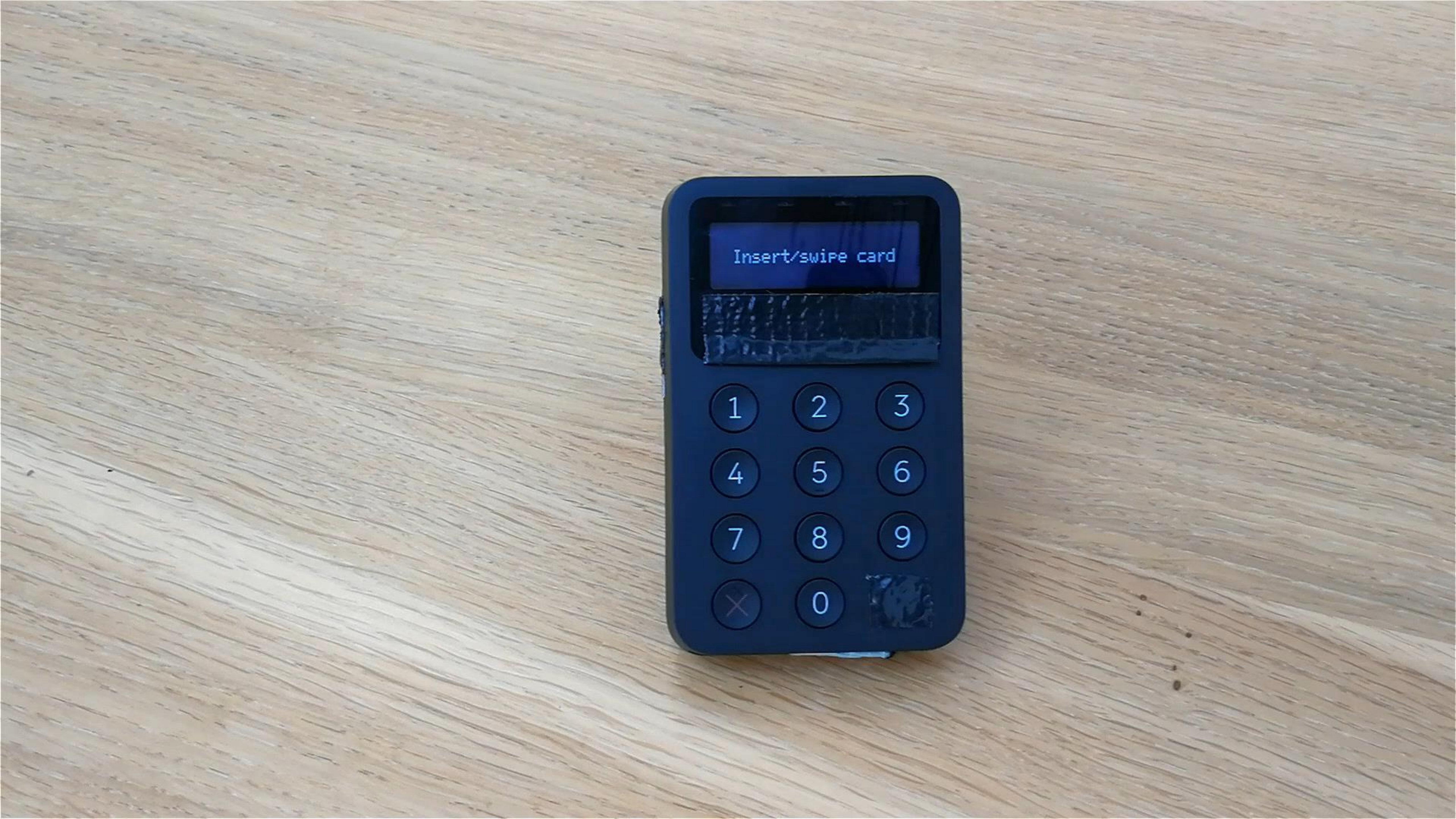



```
∨ Bluetooth RFCOMM Protocol
  ∨ Address: E/A flag: 1, C/R flag: 1, Direction: 0, Channel: 1
    ∨ 0000 10.. = DLCI: 0x02 (Direction: 0, Channel: 1)
        0000 1... = Channel: 1
        .... .0.. = Direction: 0x0
      .... ..1. = C/R Flag: Command (0x1)
      .... ...1 = EA Flag: Last field octet (0x1)
  ∨ Control: Frame type: Unnumbered Information with Header check (UIH) (0xef), P/F flag: 0
      ...0 .... = P/F flag: 0x0
      111. 1111 = Frame type: Unnumbered Information with Header check (UIH) (0xef)
    Payload length: 32
    Frame Check Sequence: 0x9a
∨ Bluetooth SPP Packet
    Data: 0d0501000017010300000c00496e736572742f7377697065...
```

Data: 0d0501000017010300000c00496e736572742f73776970652063617264440d0a

Findings

LEADING PART	MESSAGE	CRC
0d0501000017	010300000c00496e736572742f73776970652063617264	44
“Insert/swipe card”		



Insert/swipe card

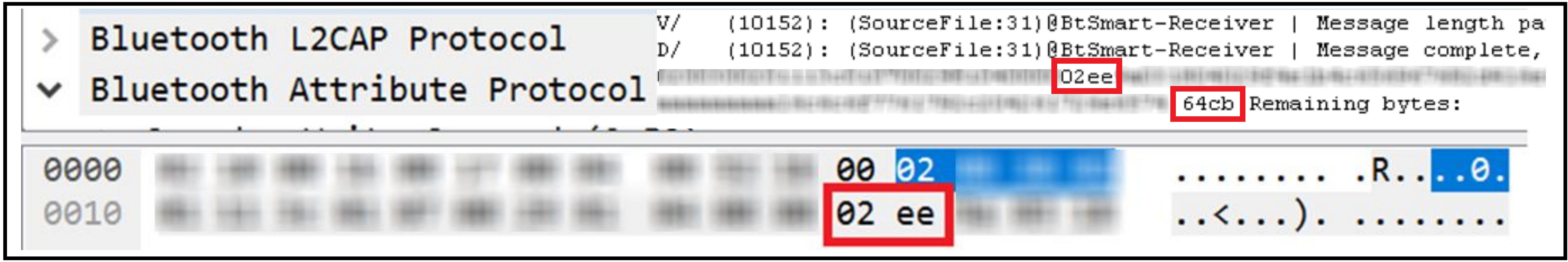
AMOUNT TAMPERING

HOW TO GET ACCESS TO TRANSACTIONS AND COMMANDS

- HTTPS
- DEVELOPER BLUETOOTH LOGS
- RE OF APK ENABLE DEBUG
- BLUETOOTH SNIFFER

HOW TO GET ACCESS TO COMMANDS

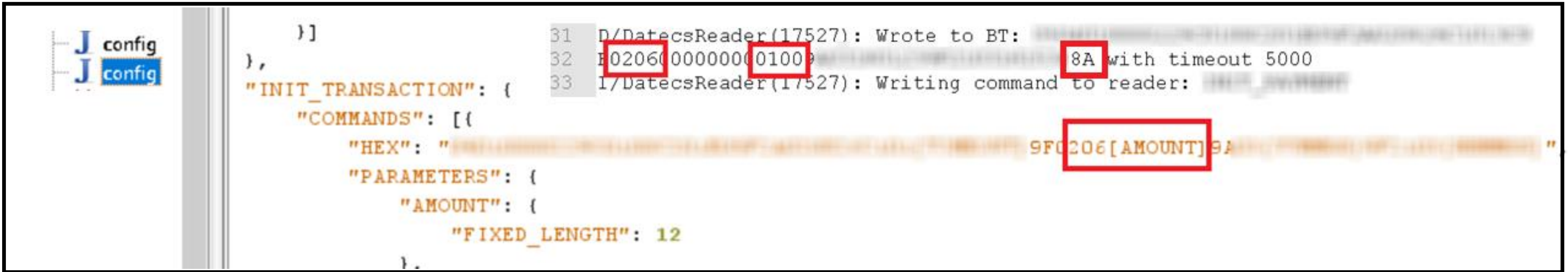
1. 0x02ee = 7.50 USD 0x64cb = checksum



```
V/    (10152): (SourceFile:31)@BtSmart-Receiver | Message length pa
D/    (10152): (SourceFile:31)@BtSmart-Receiver | Message complete,
[redacted]02ee[redacted]
[redacted] 64cb Remaining bytes:
```

```
0000  [redacted] 00 02 [redacted]   ......... .R....0.
0010  [redacted] 02 ee [redacted]   ..<...). .........
```

2. 0100 = 1.00 USD 0x8a = checksum

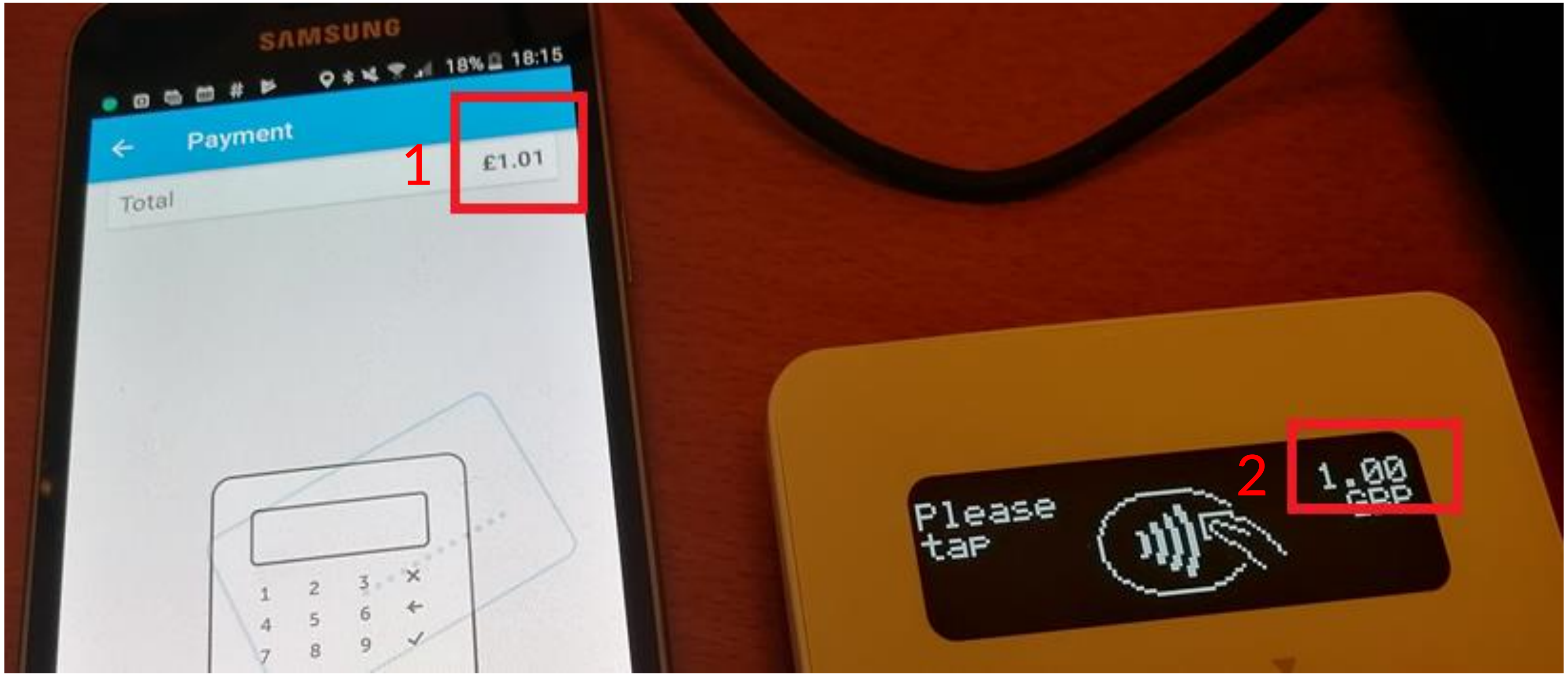


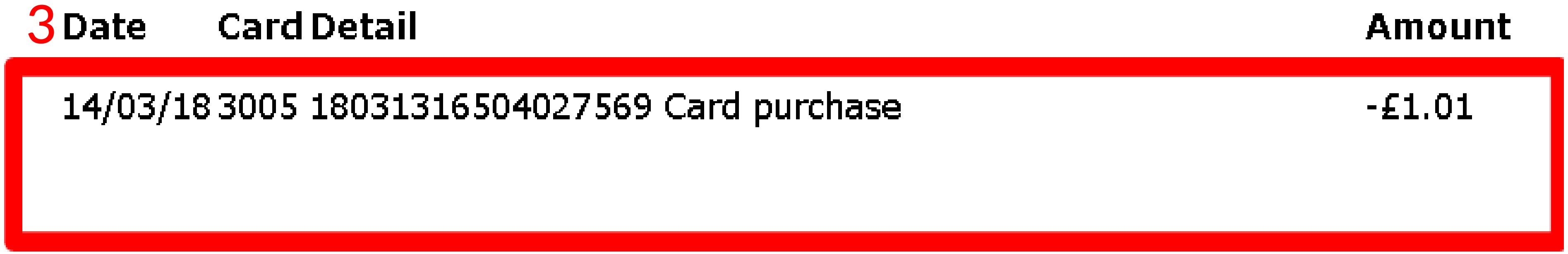
```
D/DatecsReader(17527): Wrote to BT: [redacted]
[redacted]0206[redacted]0000000[redacted]0100[redacted]8A with timeout 5000
I/DatecsReader(17527): Writing command to reader: [redacted]
```

```
    }]
},
"INIT_TRANSACTION": {
    "COMMANDS": [{
        "HEX": "[redacted]9F[redacted]206[AMOUNT][redacted]",
        "PARAMETERS": {
            "AMOUNT": {
                "FIXED_LENGTH": 12
            },
```

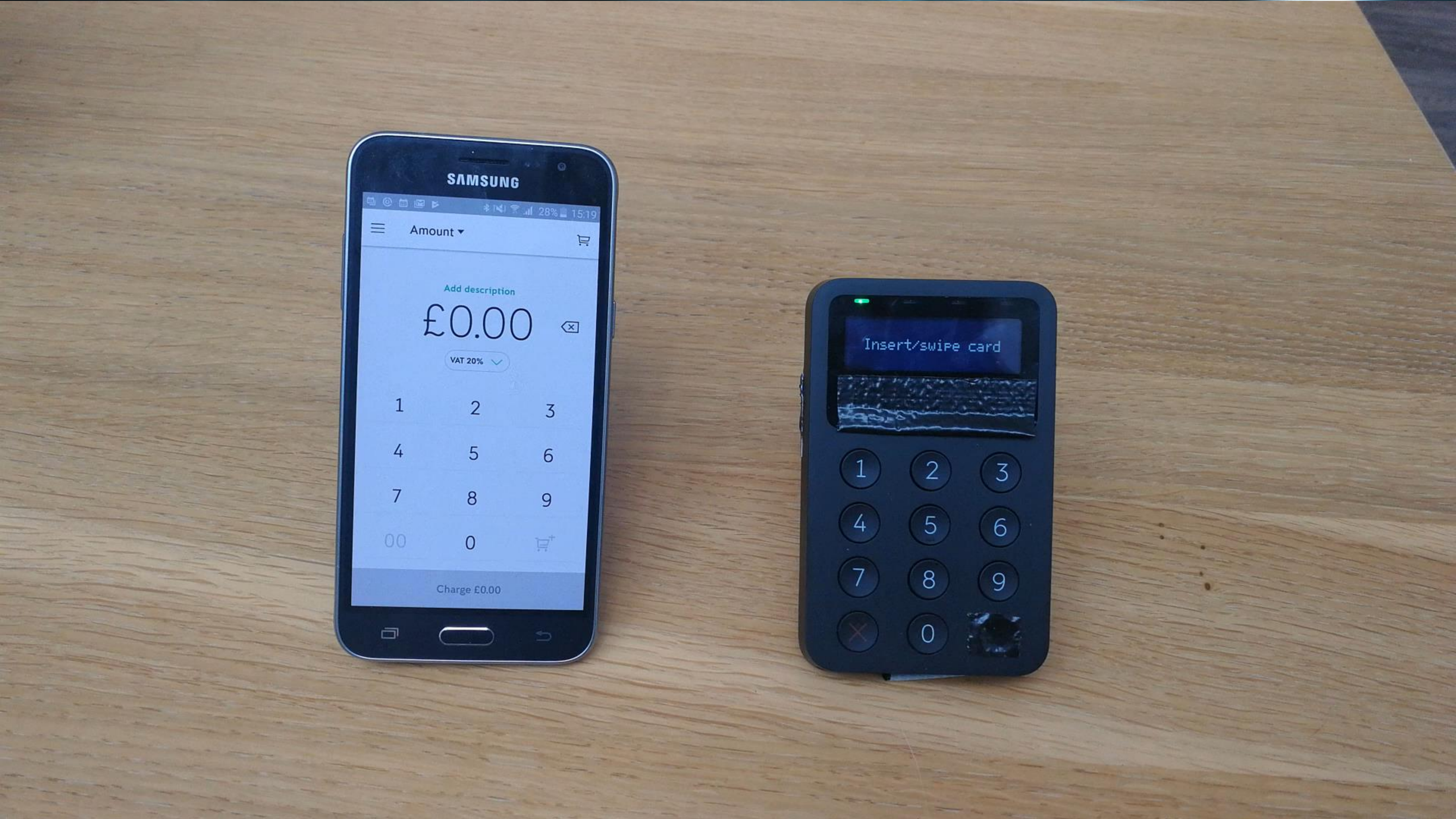
MODIFYING PAYMENT AMOUNT

1. Modified payment value
2. Original (lower) amount displayed on card reader for the customer
3. Card statement showing higher authorised transaction amount




3

Date	Card Detail	Amount
14/03/18	3005 18031316504027569 Card purchase	-£1.01

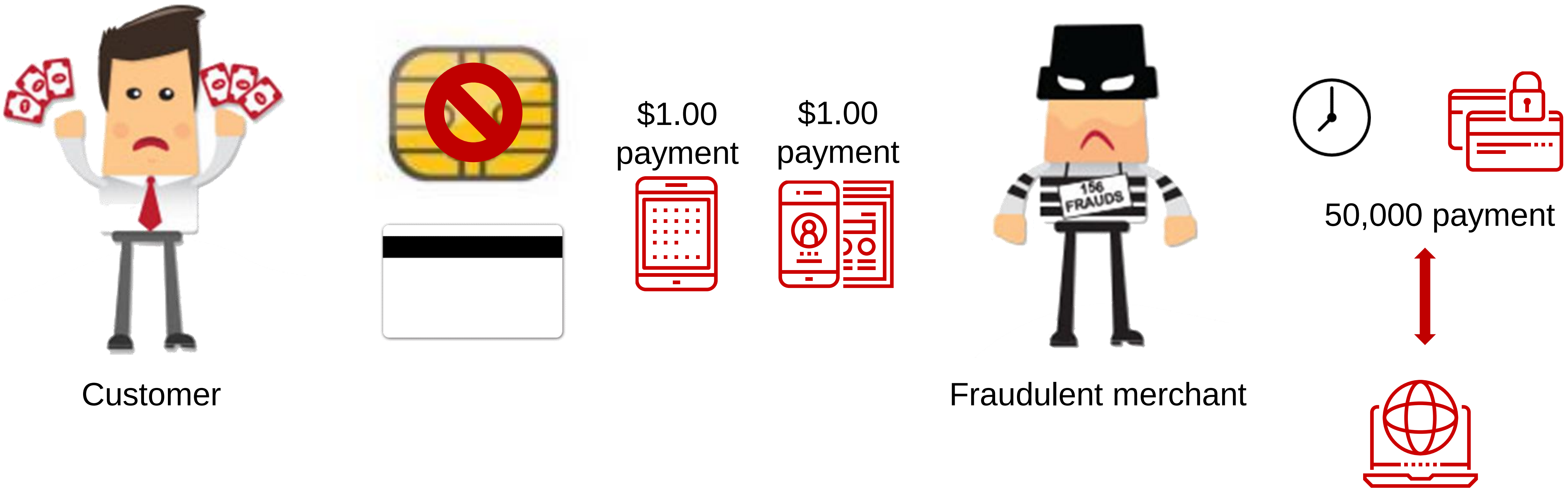

SAMSUNG
28% 15:19
Amount
Add description
£0.00
VAT 20%
1
2
3
4
5
6
7
8
9
00
0
Charge £0.00
Insert/swipe card
1
2
3
4
5
6
7
8
9
0

MODIFYING PAYMENT AMOUNT

TYPE OF PAYMENT	AMOUNT TAMPERING	SECURITY MECHANISMS
MAG-STRIPE	TRACK2	----
CONTACTLESS	POSSIBLE	AMOUNT CAN BE STORED IN CRYPTOGRAM
CHIP AND PIN	-----	AMOUNT IS STORED IN CRYPTOGRAM

LIMIT PER TRANSACTION: 50,000 USD

ATTACK



Customer

$1.00 payment

$1.00 payment

Fraudulent merchant

50,000 payment

Service Provider

MITIGATION ACTIONS FOR SERVICE PROVIDERS

- REQUEST SOLUTION FROM VENDOR
- CONTROL YOUR ECOSYSTEM
- NO MAG-STRIPE

REMOTE CODE EXECUTION

RCE = 1 REVERSE ENGINEER + 1 FIRMWARE

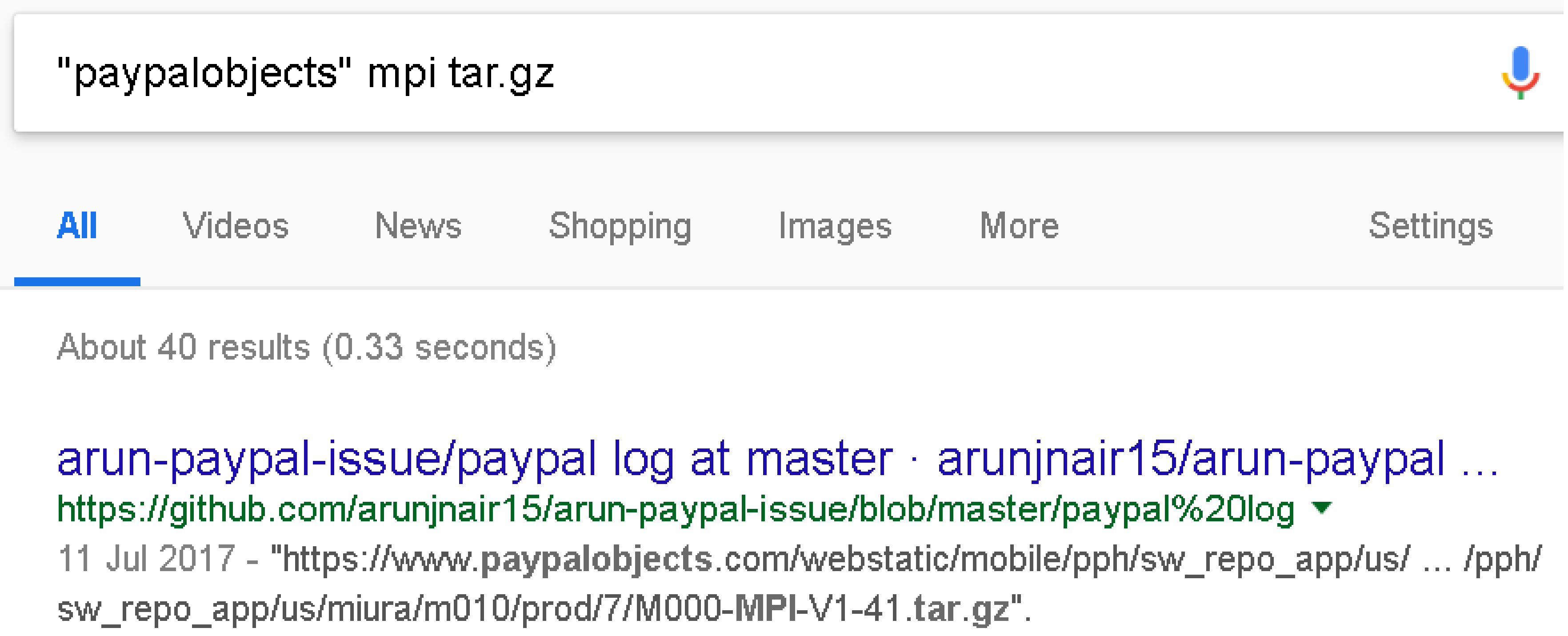
HOW FIRMWARE ARRIVES ON THE READER

https://frw.******.com/_prod_app_1_0_1_5.bin
https://frw.******.com/_prod_app_1_0_1_5.sig

https://frw.******.com/_prod_app_1_0_1_4.bin
https://frw.******.com/_prod_app_1_0_1_4.sig

Header	- RSA-2048 signature *(0x00 - 0x100)*
Body	- AES-ECB encrypted

HOW FIRMWARE ARRIVES ON THE READER



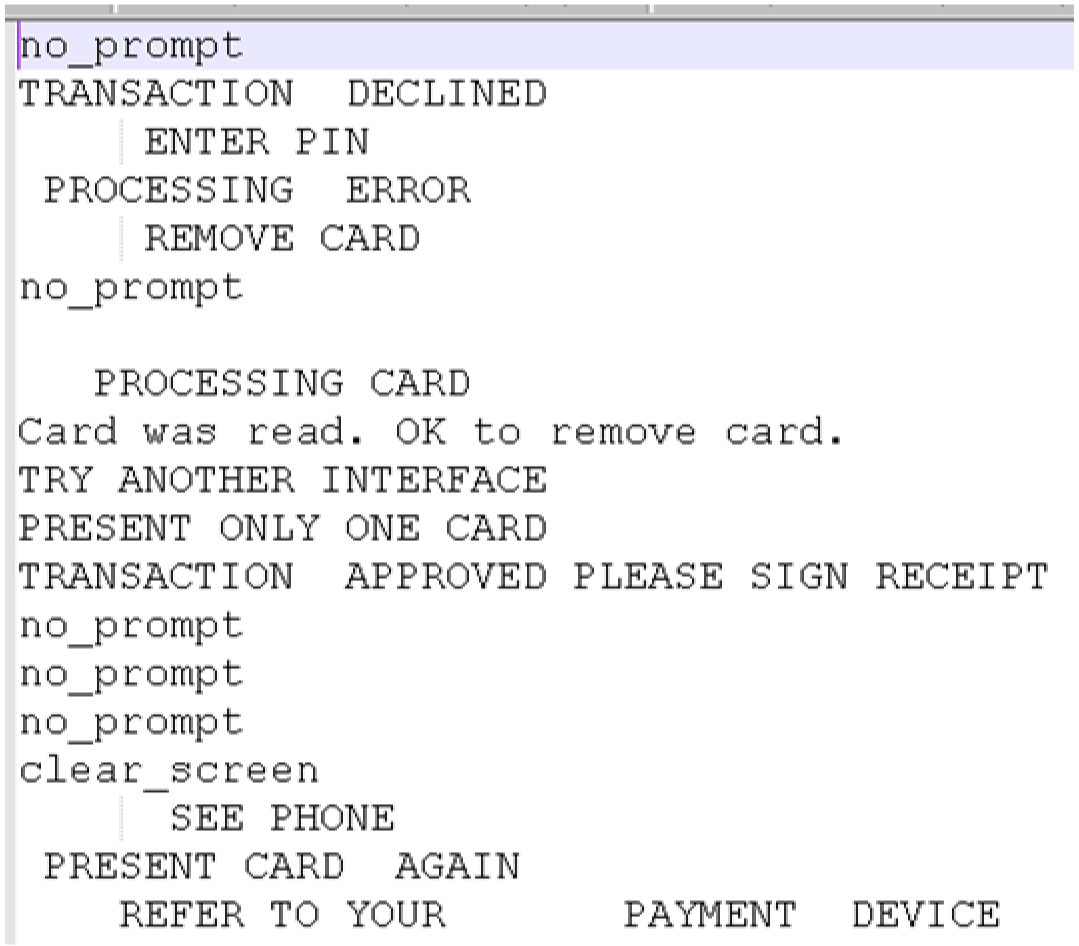
"paypalobjects" mpi tar.gz

About 40 results (0.33 seconds)

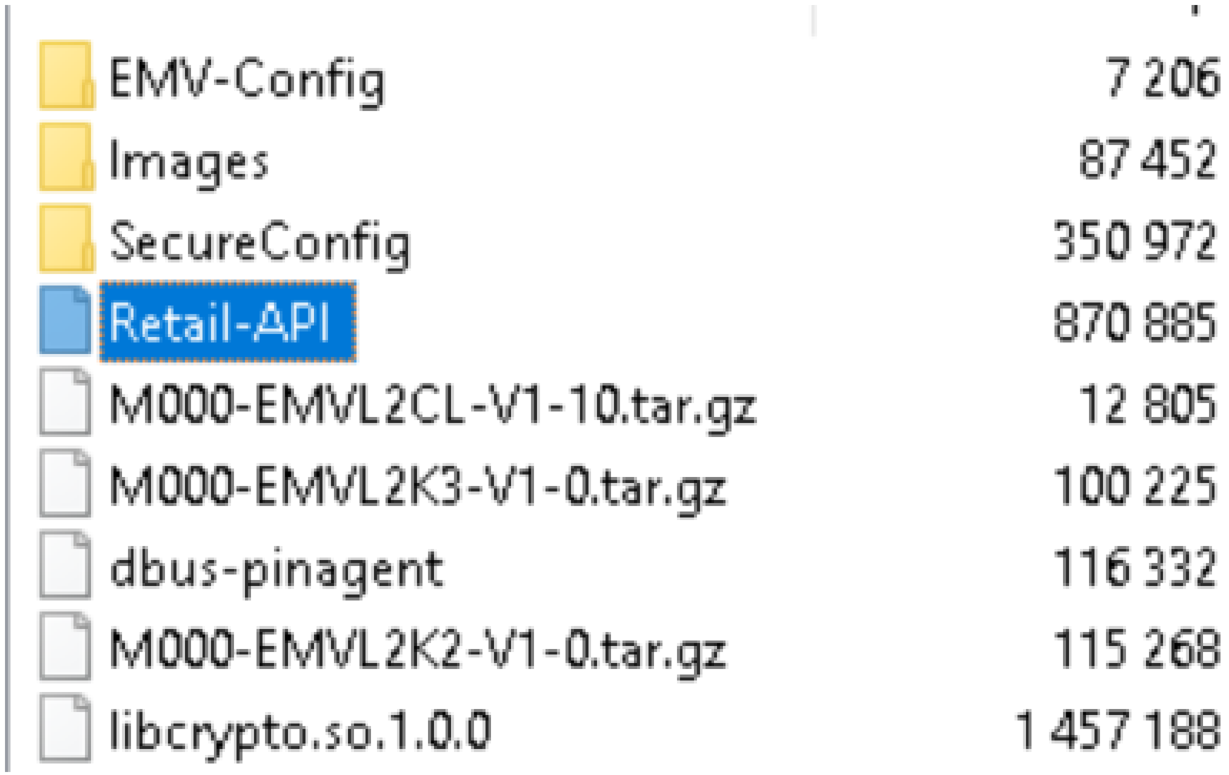
arun-paypal-issue/paypal log at master · arunjnair15/arun-paypal ...
https://github.com/arunjnair15/arun-paypal-issue/blob/master/paypal%20log
11 Jul 2017 - "https://www.**paypalobjects**.com/webstatic/mobile/pph/sw_repo_app/us/ ... /pph/sw_repo_app/us/miura/m010/prod/7/M000-**MPI**-V1-41.**tar.gz**".

https://www.paypalobjects.com/webstatic/mobile/pph/sw_repo_app/us/miura/m010/prod/7/M000-MPI-V1-41.tar.gz
https://www.paypalobjects.com/webstatic/mobile/pph/sw_repo_app/us/miura/m010/prod/7/M000-MPI-V1-39.tar.gz

HOW FIRMWARE ARRIVES ON THE READER

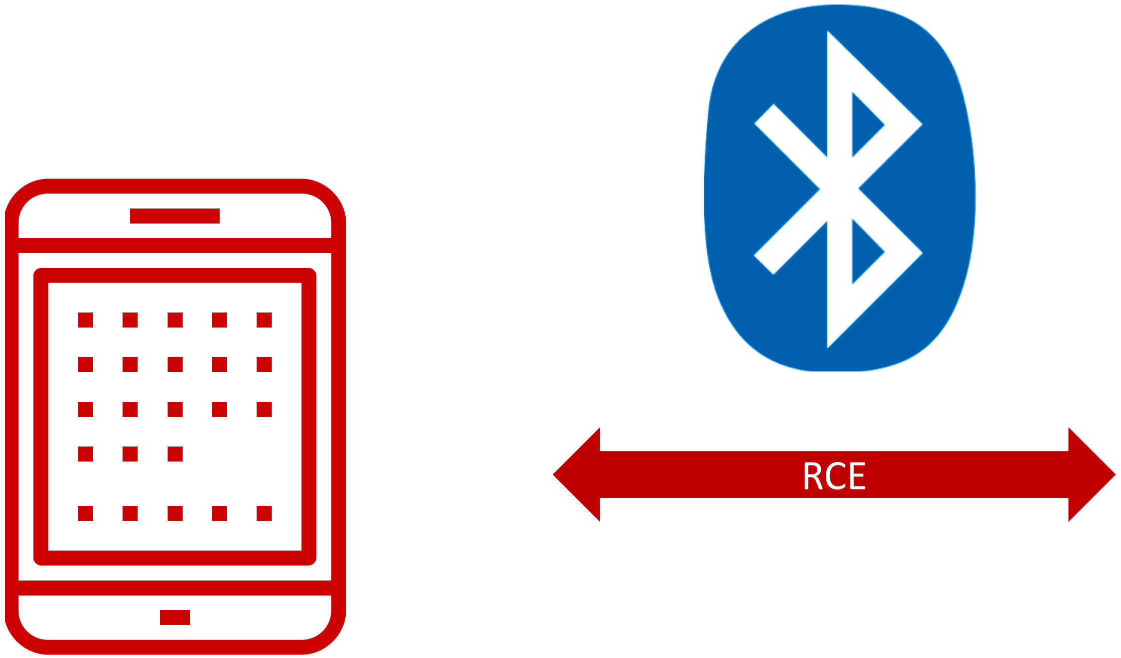


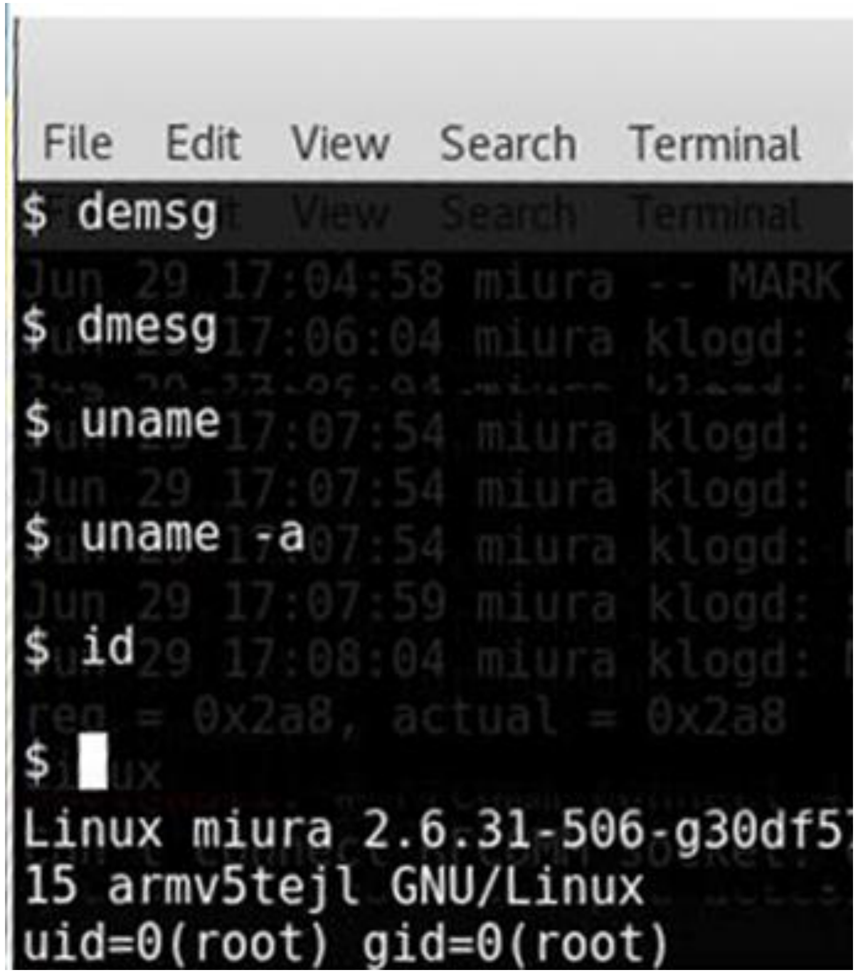
```
no_prompt
TRANSACTION  DECLINED
     ENTER PIN
 PROCESSING  ERROR
     REMOVE CARD
no_prompt

   PROCESSING CARD
Card was read. OK to remove card.
TRY ANOTHER INTERFACE
PRESENT ONLY ONE CARD
TRANSACTION  APPROVED PLEASE SIGN RECEIPT
no_prompt
no_prompt
no_prompt
clear_screen
      SEE PHONE
 PRESENT CARD  AGAIN
    REFER TO YOUR       PAYMENT  DEVICE
```



EMV-Config	7 206
Images	87 452
SecureConfig	350 972
Retail-API	870 885
M000-EMVL2CL-V1-10.tar.gz	12 805
M000-EMVL2K3-V1-0.tar.gz	100 225
dbus-pinagent	116 332
M000-EMVL2K2-V1-0.tar.gz	115 268
libcrypto.so.1.0.0	1 457 188

HOW FIRMWARE ARRIVES ON THE READER





```
$ demsg
$ dmesg
$ uname
$ uname -a
$ id
$ █
Linux miura 2.6.31-506-g30df5
15 armv5tejl GNU/Linux
uid=0(root) gid=0(root)
```

INFECTED MPOS

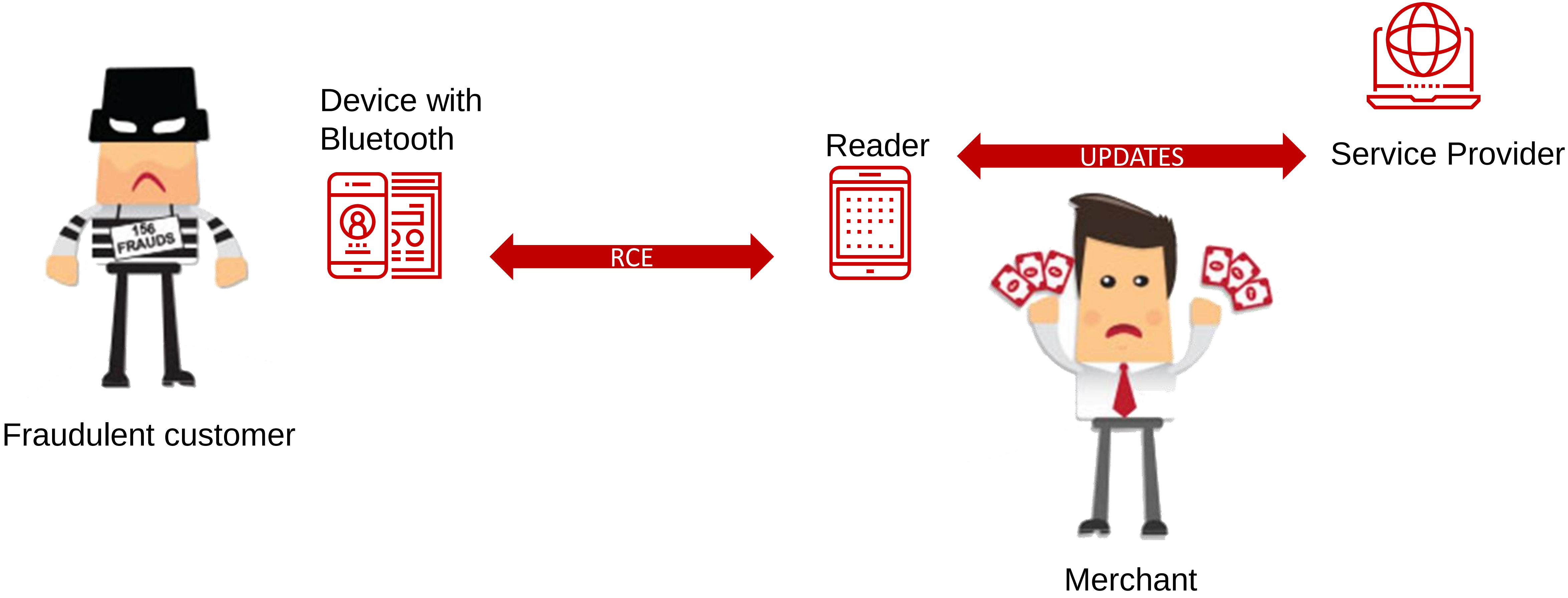
- PAYMENT ATTACKS
- COLLECT TRACK 2/PIN
- PAYMENT RESEARCH

DEVICE PERSISTENCE

REBOOT

GAME OVER

ATTACK



Device with Bluetooth

RCE

Reader

UPDATES

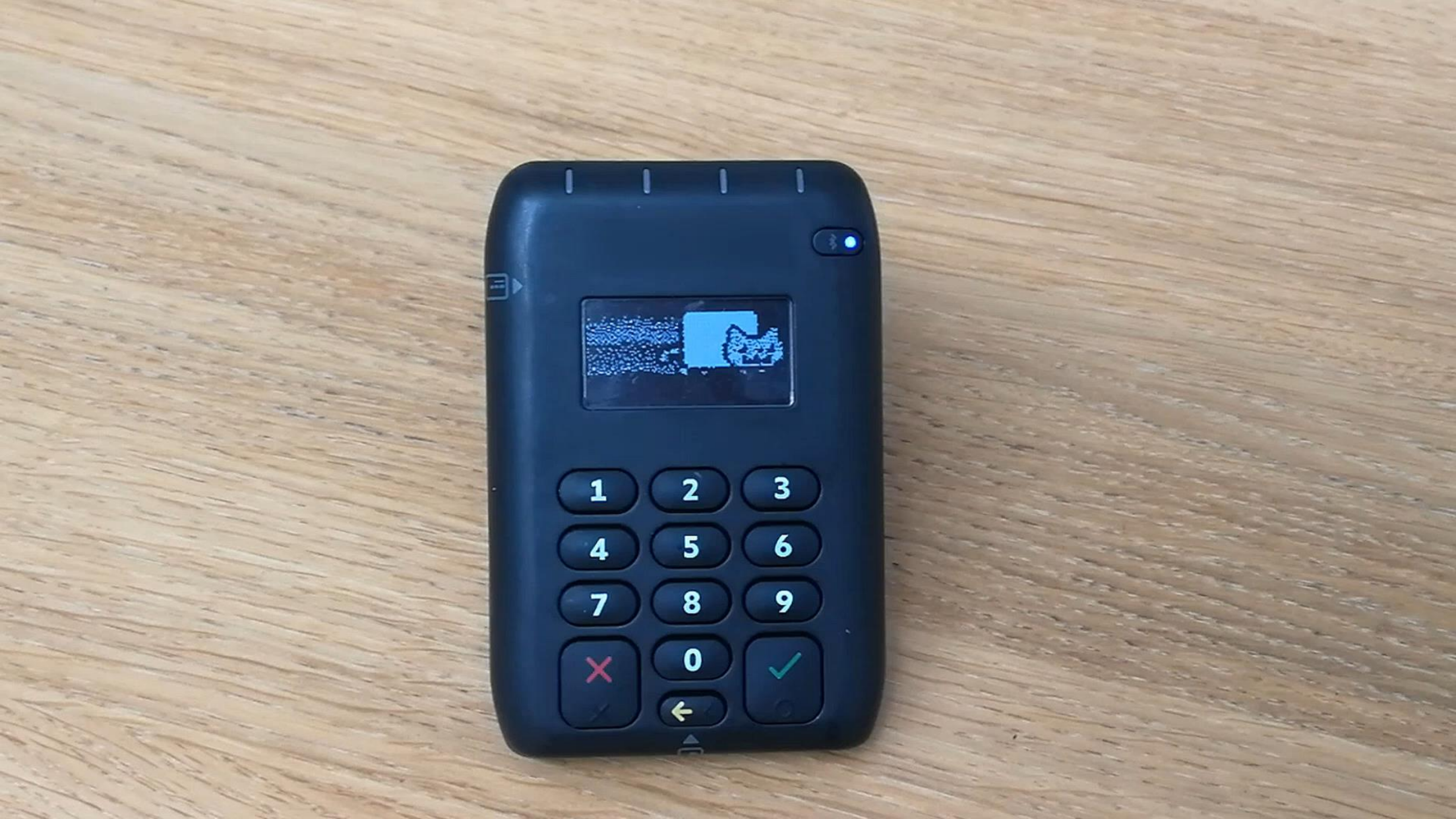
Service Provider

Fraudulent customer

Merchant

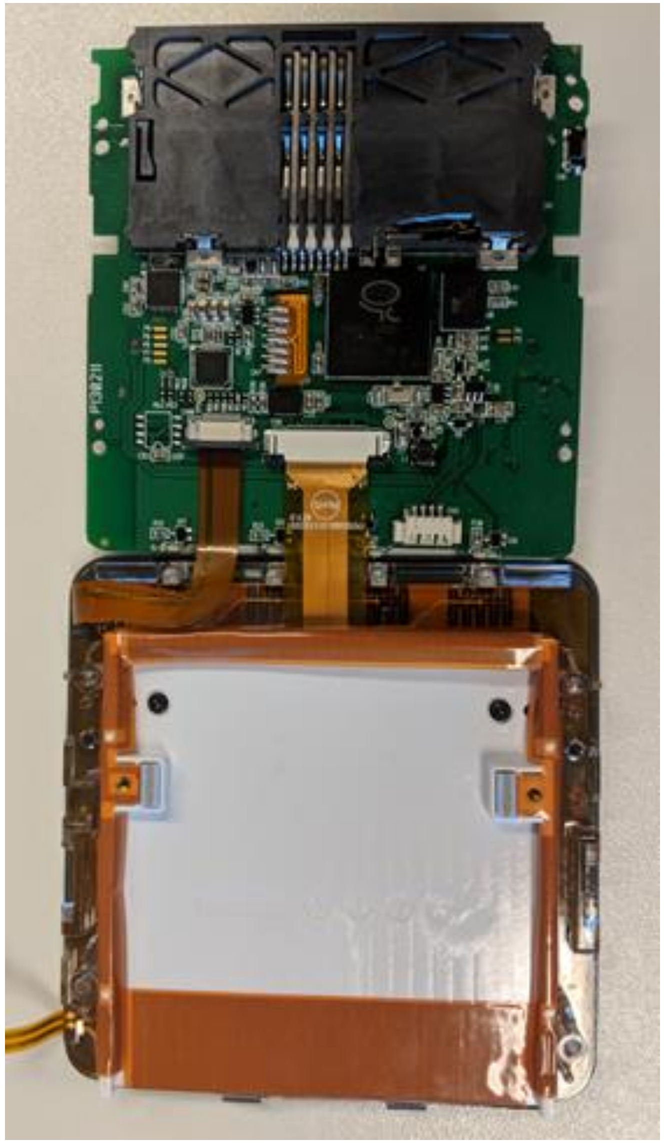
MITIGATIONS

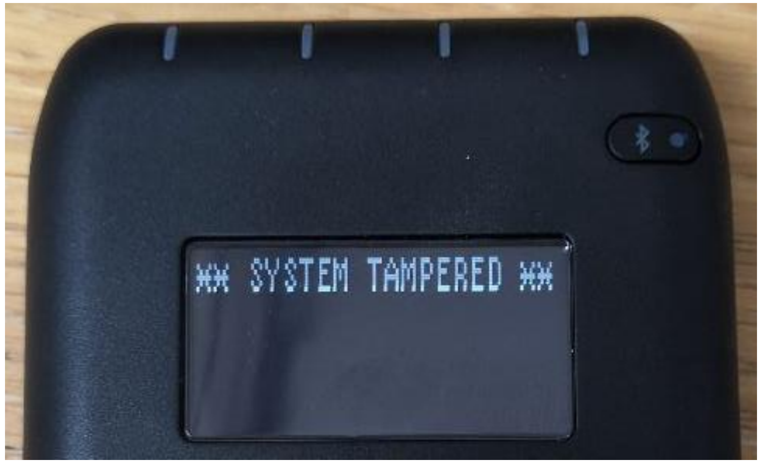
- NO VULNERABLE OR OUT-OF-DATE FIRMWARE
- NO DOWNGRADES
- PREVENTATIVE MONITORING

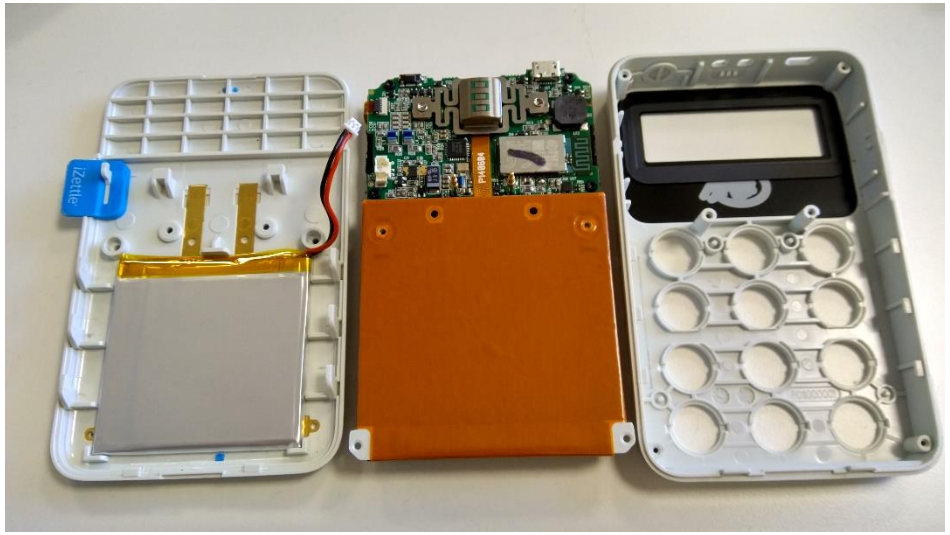


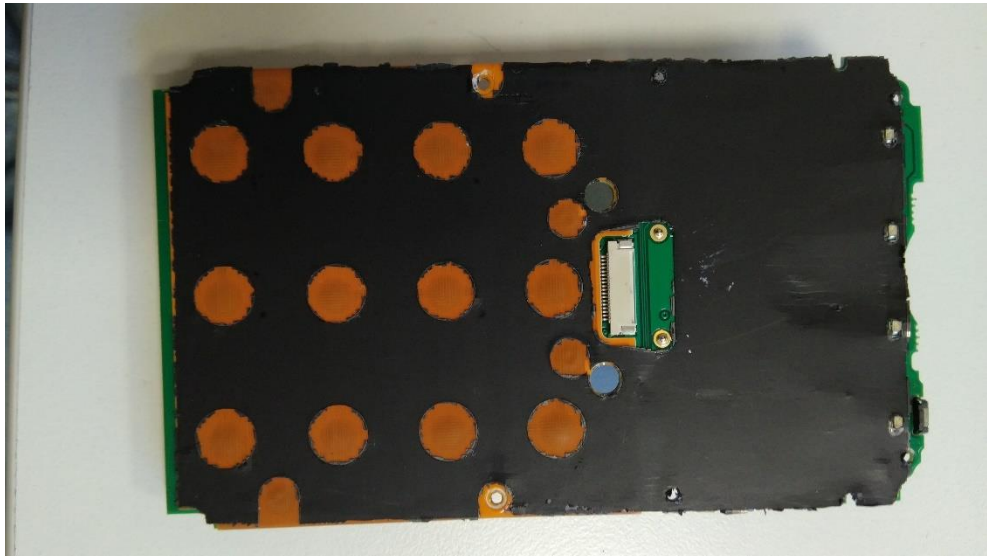
1
2
3
4
5
6
7
8
9
0

HARDWARE OBSERVATIONS









SECONDARY FACTORS

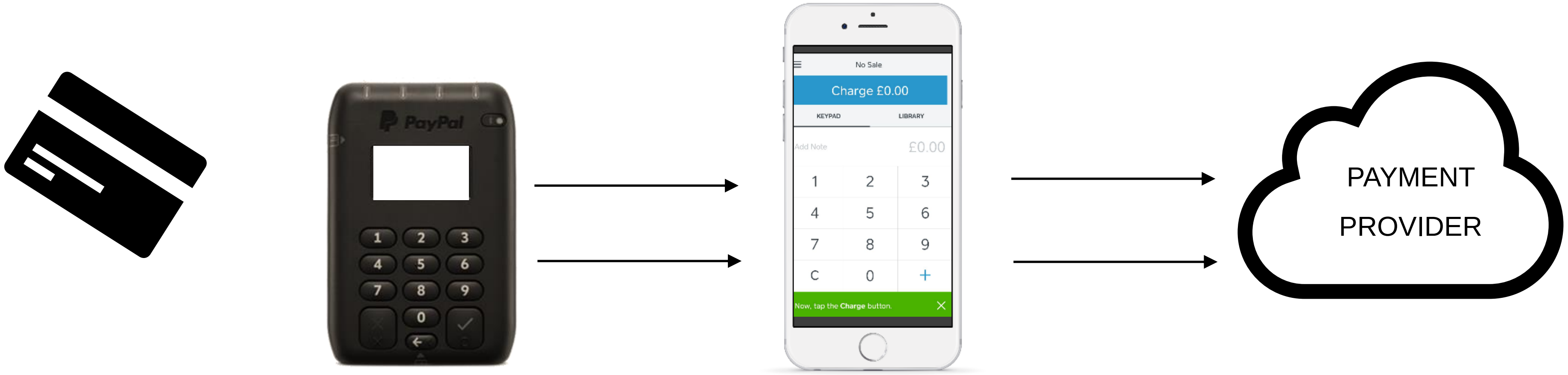
- ✓ ENROLMENT PROCESS
- ✓ ON BOARDING CHECKS VS TRANSACTION MONITORING
- ✓ DIFFERENCES IN GEO – MSD, OFFLINE PROCESSING
- ✓ WHAT SHOULD BE CONSIDERED AN ACCEPTED RISK?
- ✓ ACCESS TO HCI LOGS/APP, LOCATION SPOOFING

Conclusions

Reader	Cost reader/Fee per transaction	Enrollment process	Antifraud + Security checks	Physical security	FW RE	Mobile Ecosystem	Arbitrary commands	Red teaming	Amount tampering
Square [EU]	$51 1.75-2.5%	Low - no anti money laundering checks but some ID checks	Strict – active monitoring of transactions	N/A	-	strict	-	-	-
Square [USA]	$50 2.5-2.75%		Strict – correlation of “bad” readers, phones and acc info	N/A	-	medium (dev)	-	+	-
Square mag-stripe [EU + USA]	Free 2.5-2.75%		Strict (see above)	Low	-	low	-	+	+ [no display]
Square miura [USA]	$130 2.5-2.75%		Strict (see above)	N/A	+	N/A	+ [via RCE]	+	+ (via RCE)
PayPal miura	$60 1-2.75%	High - anti-money laundering checks + credit check (to take out credit agreement)	Strict – transaction monitoring	N/A	+	low	+ [via RCE]	+	+ (via RCE)
SumUp	$40 1.69%			Medium	-	low	+	+	+
iZettle datecs	$40 1.75%	Medium - ant-money laundering check + ID checks	Low – limited monitoring, on finding suspect activity block withdrawal - acc otherwise active	High	-	low	+	-	+

MPOS FOR RED TEAMING

1. Carry out an assessment of reader to gather preliminary data + info from cards.
2. Use data to carry out normal transactions to obtain baseline.
3. Use info obtained during this process to identify potential weaknesses and vulnerabilities.
4. Carry out “modified” transactions



PAYMENT PROVIDER

ASSESSING RISK - WHAT DOES THIS MEAN FOR YOUR BUSINESS?

Conclusions

CONCLUSIONS

RECOMMENDATIONS FOR MPOS MANUFACTURERS

- Control firmware versions, encrypt & sign firmware
- Use Bluetooth pairing mode that provides visual confirmation of reader/phone pairing such as pass key entry
- Integrate security testing into the development process
- Implement user authentication and input sanitisation at the application level

CONCLUSIONS

RECOMMENDATIONS FOR MPOS VENDORS

- Protect deprecated protocols such as mag-stripe
- Use preventive monitoring as a best practice
- Don’t allow use of vulnerable or out-of-date firmware, prohibit downgrades
- Place more emphasis on enrolment checks
- Protect the mobile ecosystem
- Implement user authentication and input sanitization at application level

CONCLUSIONS

RECOMMENDATIONS FOR MPOS MERCHANTS

- Control physical access to devices
- Do not use mag-stripe transactions

- Assess the mPOS ecosystem
- Choose a vendor who places emphasis on protecting whole ecosystem

THANKS

Leigh-Anne Galloway

@L_AGalloway

Tim Yunusov

@a66at

Hardware and firmware:
Artem Ivachev

Hardware observations:
Alexey Stennikov
Maxim Goryachy
Mark Carney