black hat EUROPE 2018

DECEMBER 3-6, 2018

EXCEL LONDON / UNITED KINGDOM

# No Free Charge Theorem 2.0

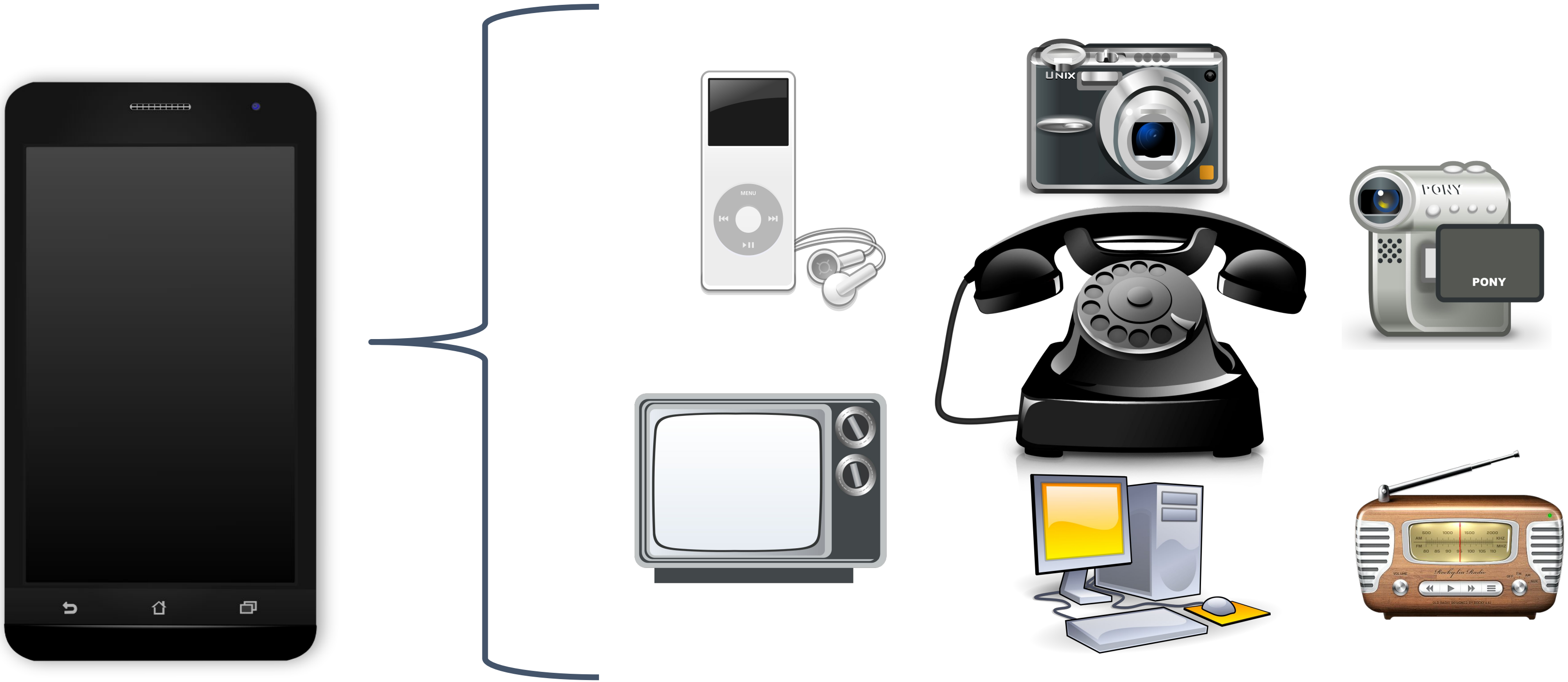
How to steal private information from a mobile device using a powerbank

**Riccardo Spolaor**
University of Oxford, UK

Riccardo Bonafede - University of Padua, IT
Veelasha Moonsamy - Utrecht University, NL
Mauro Conti - University of Padua, IT

***Disclaimer**: All logos, photos, etc. used in this presentation are the property of their respective copyright owners and are used here for educational purposes only.*

# Smartphones are amazing!



# Our travel companion

How did you arrive here?

Let me guess…

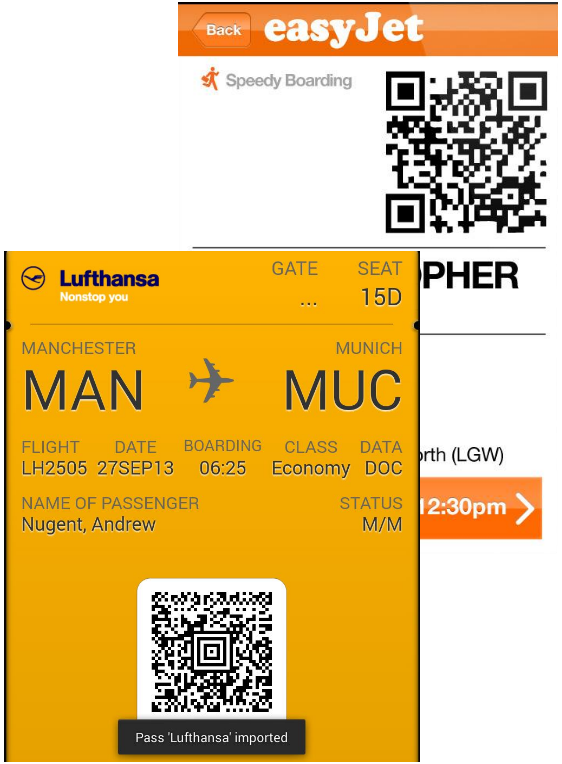
# Our travel companion

By plane?

Lufthansa

Emirates

BRITISH AIRWAYS



PHER

rth (LGW)

12:30pm

Lufthansa
Nonstop you

| GATE | SEAT |
|---|---|
| ... | 15D |

MANCHESTER MAN → MUNICH MUC

| FLIGHT | DATE | BOARDING | CLASS | DATA |
|---|---|---|---|---|
| LH2505 | 27SEP13 | 06:25 | Economy | DOC |

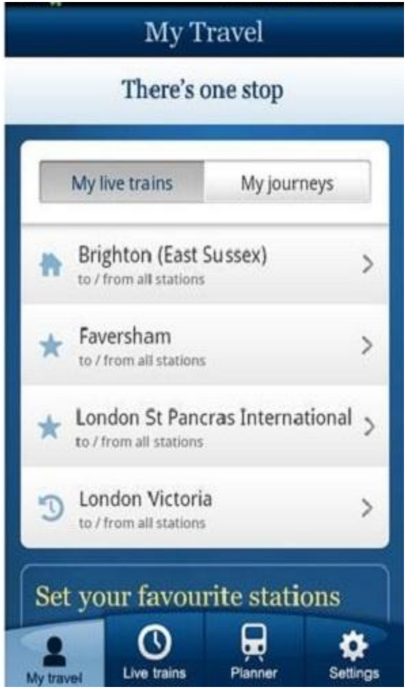
| NAME OF PASSENGER | STATUS |
|---|---|
| Nugent, Andrew | M/M |

Pass 'Lufthansa' imported

# Our travel companion

By train/tube?

LONDON TUBE



My Travel

There's one stop

Brighton (East Sussex)
to / from all stations

Faversham
to / from all stations

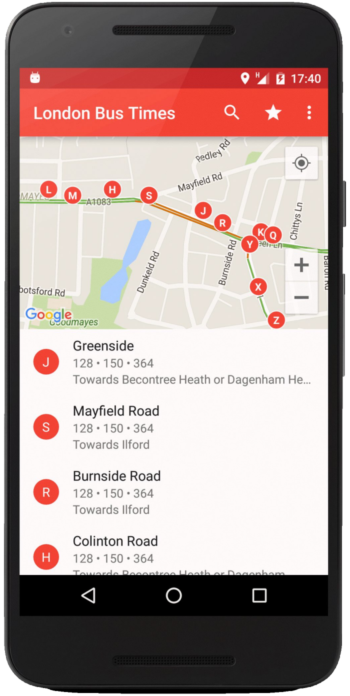
London St Pancras International
to / from all stations

London Victoria
to / from all stations

Set your favourite stations

# Our travel companion

By bus?



J Greenside
128 • 150 • 364
Towards Becontree Heath or Dagenham He...

S Mayfield Road
128 • 150 • 364
Towards Ilford

R Burnside Road
128 • 150 • 364
Towards Ilford

H Colinton Road
128 • 150 • 364
Towards Becontree Heath or Dagenham

# Our travel companion

By cab/ride?

Booking

Jai Amby Nagar, Tonk, Jaipur | Add details

Rajat Path, Mansarovar, Jaipur | Estimate Rs(150-157)

Cash | Promo code

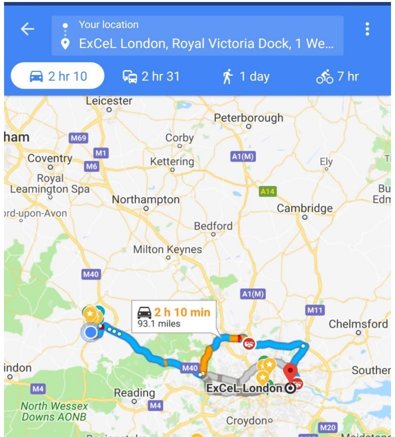
Confirm Booking!

App-a-Cab

UBER

# Our travel companion

## By car?

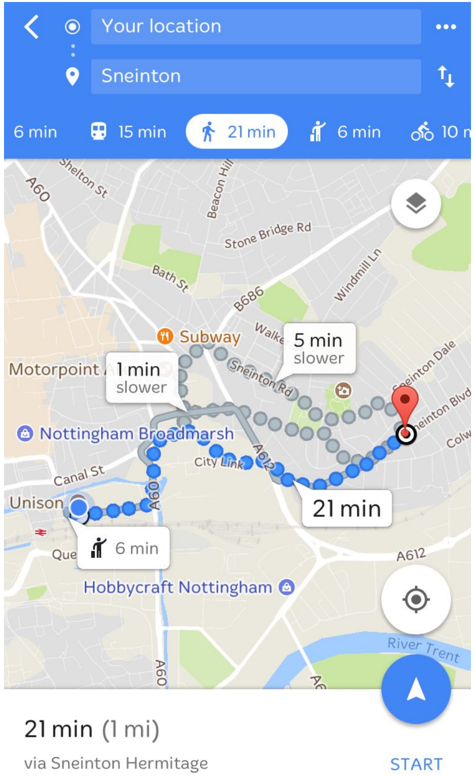

Your location
ExCeL London, Royal Victoria Dock, 1 We...
2 hr 10
2 hr 31
1 day
7 hr

2 h 10 min (93.1 miles)

Via M40 and M25

# Our travel companion

On foot?


Your location

Sneinton

6 min | 15 min | 21 min | 6 min | 10 m

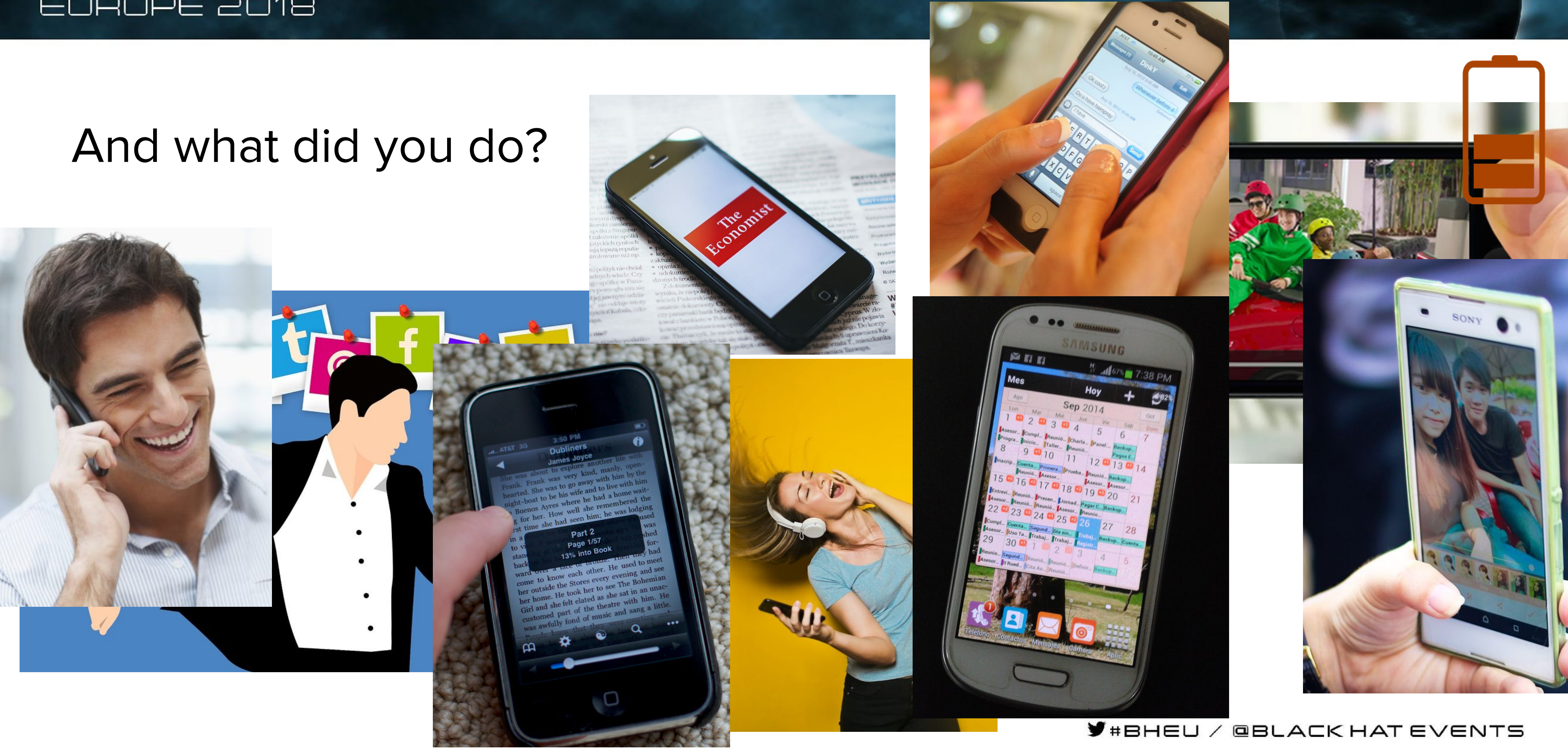
21 min (1 mi)

via Sneinton Hermitage

START

# Our door to the world

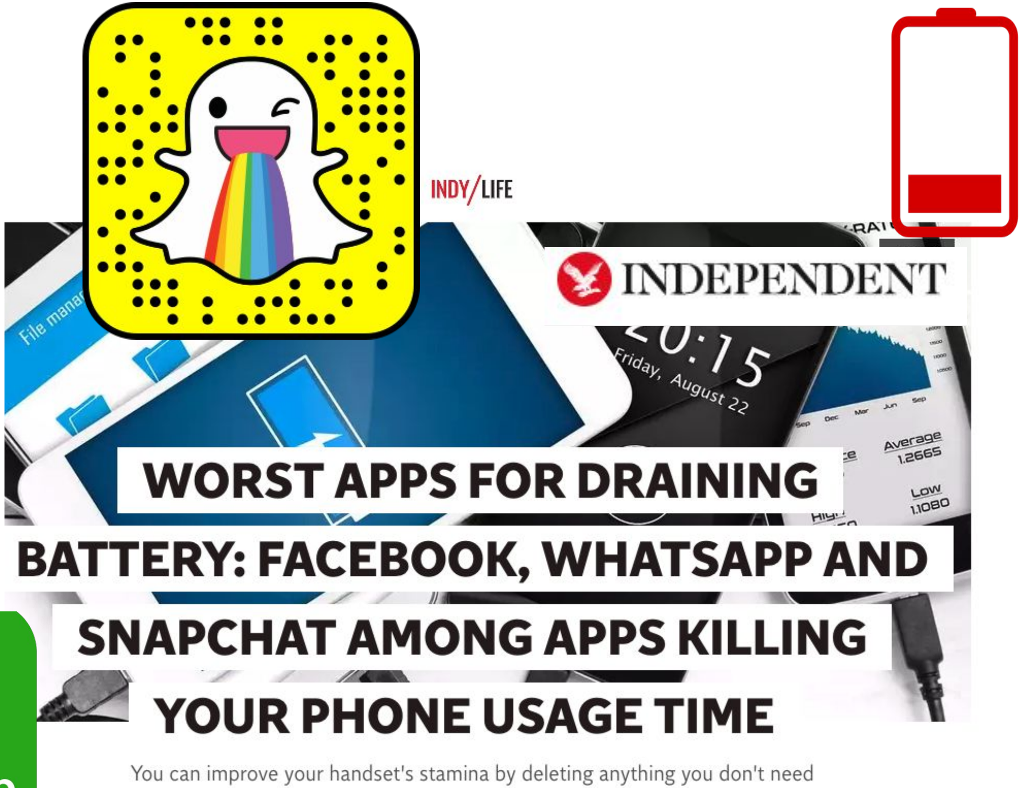
And what did you do?



# Battery: its weak point

But it is not enough!

We have "Battery killer" apps



INDY/LIFE

INDEPENDENT

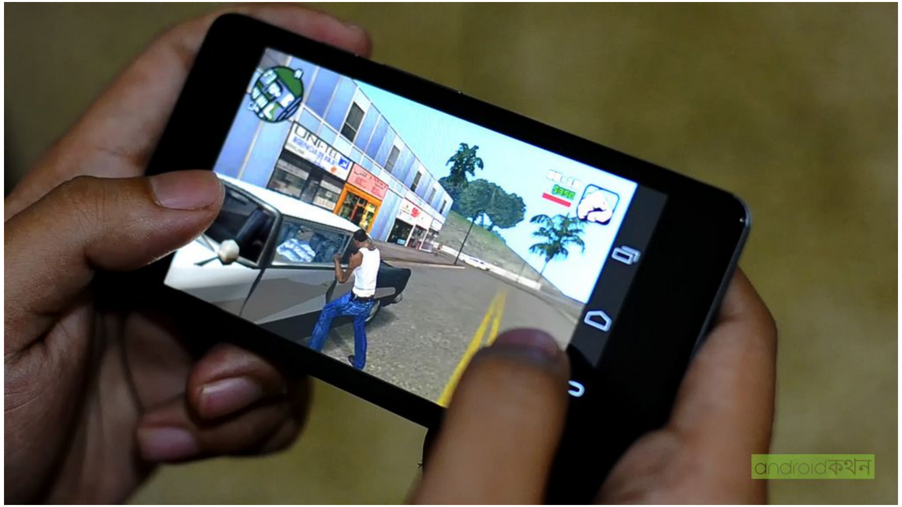
WORST APPS FOR DRAINING BATTERY: FACEBOOK, WHATSAPP AND SNAPCHAT AMONG APPS KILLING YOUR PHONE USAGE TIME

You can improve your handset's stamina by deleting anything you don't need

# Battery: its weak point

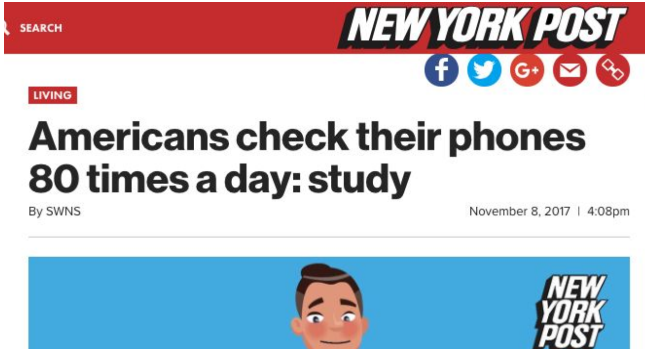
But it is not enough!

We have “Battery killer” apps



# Low Battery

Smartphones are amazing!
…but addictive!



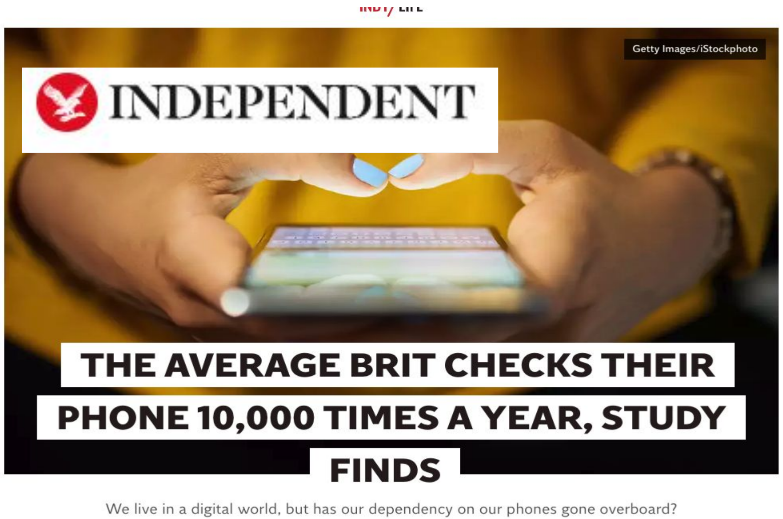
SEARCH NEW YORK POST

LIVING

## Americans check their phones 80 times a day: study

By SWNS

November 8, 2017 | 4:08pm



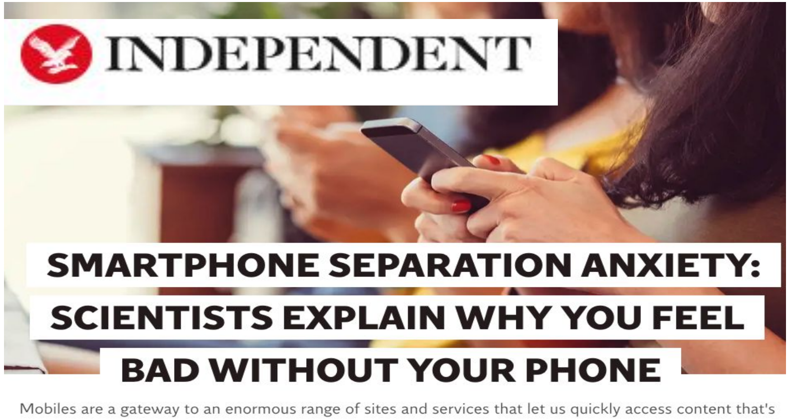
INDY/ LIFE

Getty Images/iStockphoto

INDEPENDENT

## THE AVERAGE BRIT CHECKS THEIR PHONE 10,000 TIMES A YEAR, STUDY FINDS

We live in a digital world, but has our dependency on our phones gone overboard?



INDEPENDENT

## SMARTPHONE SEPARATION ANXIETY: SCIENTISTS EXPLAIN WHY YOU FEEL BAD WITHOUT YOUR PHONE

Mobiles are a gateway to an enormous range of sites and services that let us quickly access content that's

# Our priorities change over time

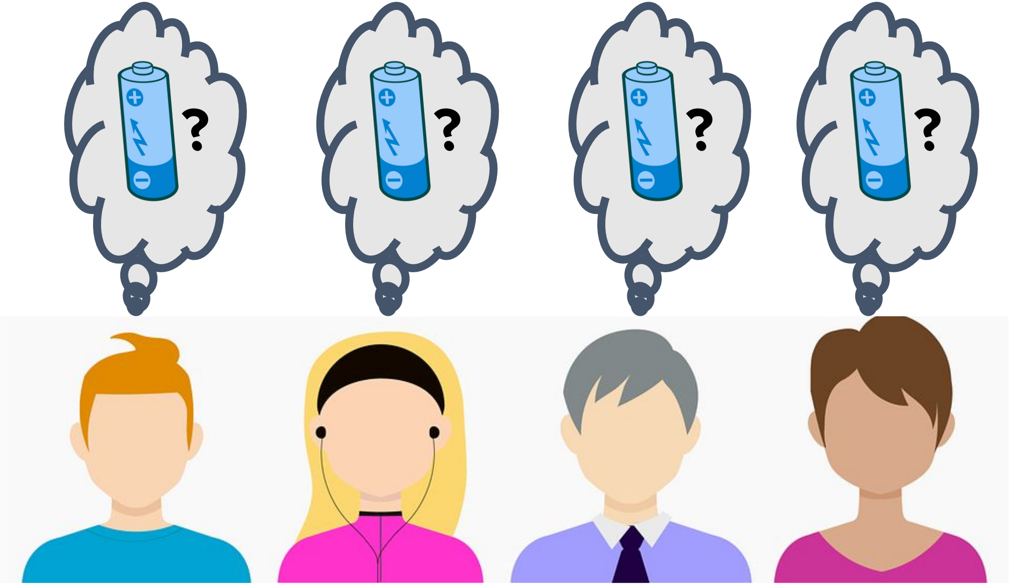
Before we were looking for Internet connectivity…

# Our priorities change over time

… now we constantly look for recharge the battery!

# … The market responds

Where there is the demand…



# … The market responds: free charging stations

Where is the demand… there is a supply

# … The market responds: USB wall sockets

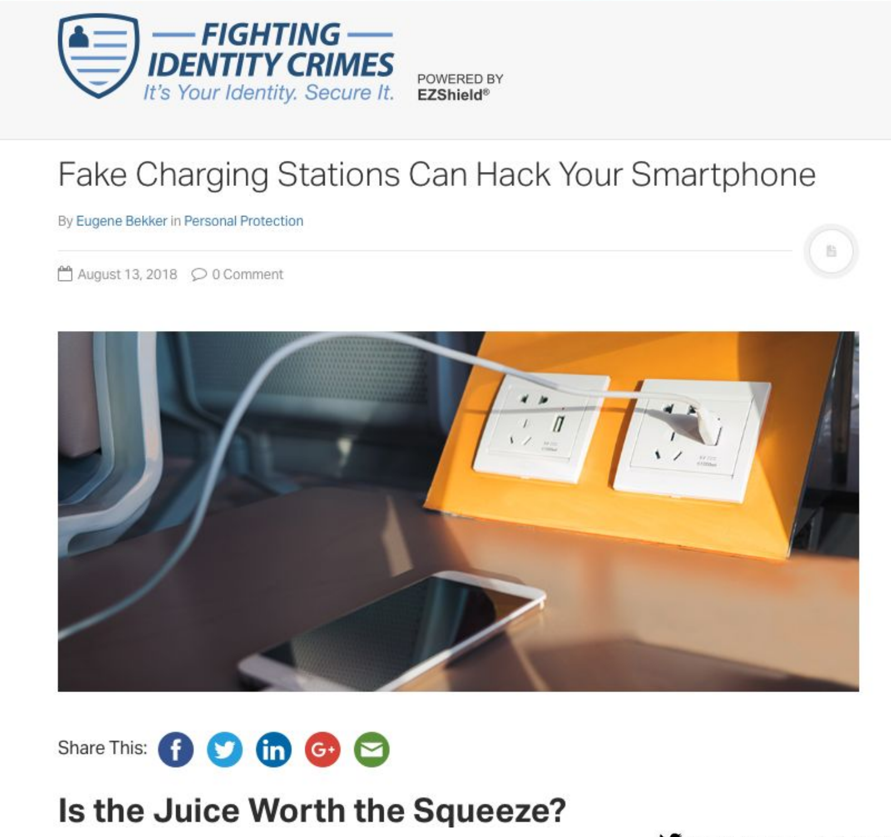
Where is the demand… there is a supply

ClearChannel AIRPORTS
neptune NETWORKS
You are at Clear Channel / DFW
FREE POWER / FREE INTERNET STATION
GATE D23
Customer Service: [redacted]
CAT-5
INTERNET CONNECTION
CAT-5 ETHERNET CABLE REQUIRED
USB CHARGING PORT

# … The market responds: power banks

Where is the demand… there is a supply

# … And the hackers strike back



FIGHTING IDENTITY CRIMES

It's Your Identity. Secure It.

POWERED BY EZShield®

## Fake Charging Stations Can Hack Your Smartphone

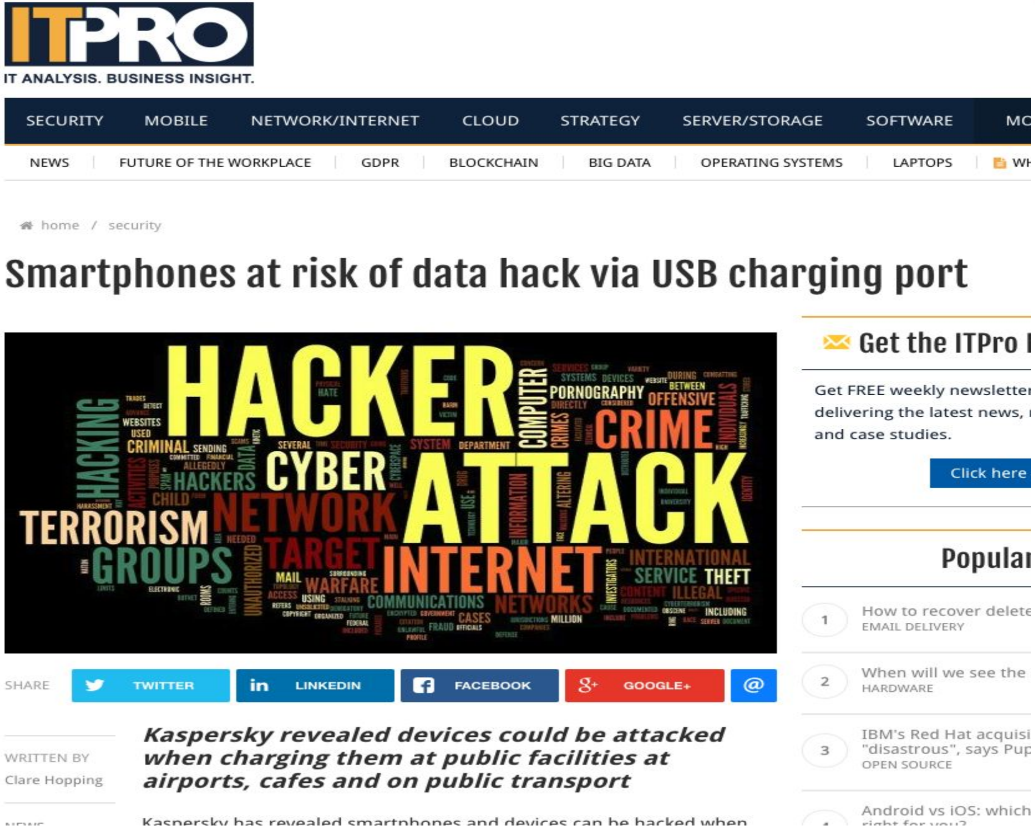
By Eugene Bekker in Personal Protection

August 13, 2018 0 Comment

Share This:

### Is the Juice Worth the Squeeze?

# … And the hackers strike back



ITPRO
IT ANALYSIS. BUSINESS INSIGHT.

SECURITY MOBILE NETWORK/INTERNET CLOUD STRATEGY SERVER/STORAGE SOFTWARE MO

NEWS | FUTURE OF THE WORKPLACE | GDPR | BLOCKCHAIN | BIG DATA | OPERATING SYSTEMS | LAPTOPS | WH

home / security

## Smartphones at risk of data hack via USB charging port

SHARE TWITTER LINKEDIN FACEBOOK GOOGLE+ @

WRITTEN BY
Clare Hopping

NEWS

***Kaspersky revealed devices could be attacked when charging them at public facilities at airports, cafes and on public transport***

Kaspersky has revealed smartphones and devices can be hacked when

Get the ITPro I

Get FREE weekly newsletter delivering the latest news, and case studies.

Click here

Popular

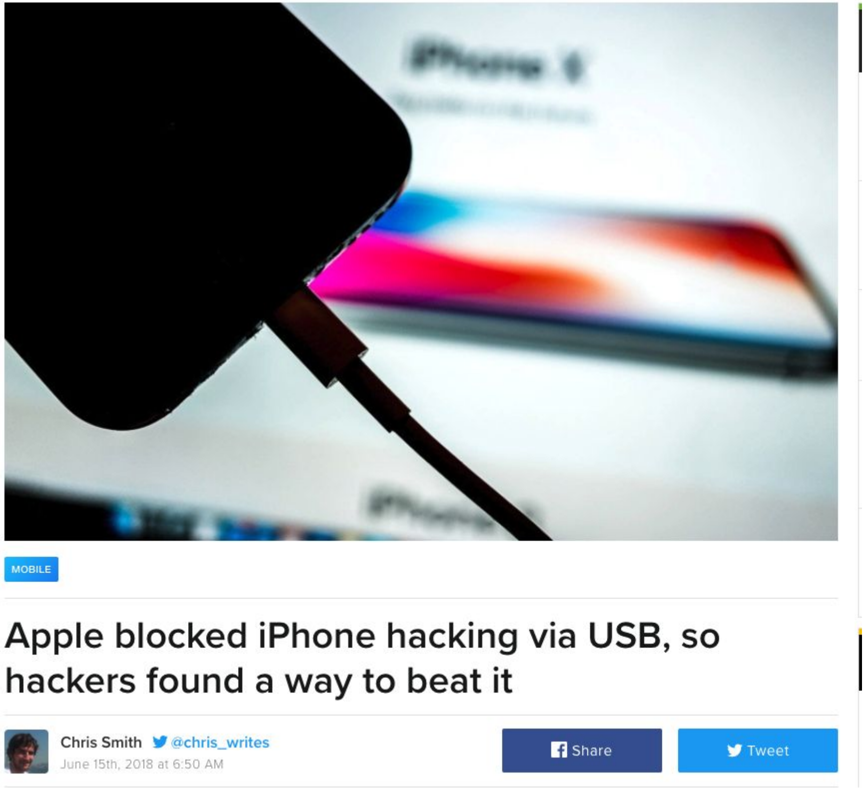
1 How to recover delete
EMAIL DELIVERY

2 When will we see the
HARDWARE

3 IBM's Red Hat acquisi "disastrous", says Pup
OPEN SOURCE

4 Android vs iOS: which right for you?

# … And the hackers strike back

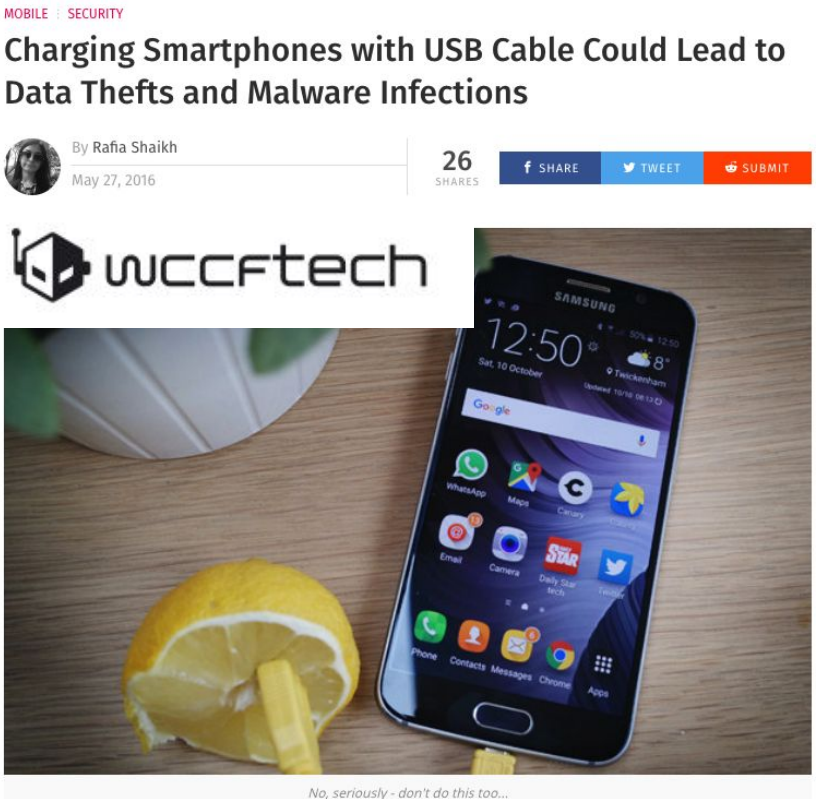


MOBILE

## Apple blocked iPhone hacking via USB, so hackers found a way to beat it

Chris Smith @chris_writes
June 15th, 2018 at 6:50 AM

# … And the hackers strike back



MOBILE | SECURITY

## Charging Smartphones with USB Cable Could Lead to Data Thefts and Malware Infections

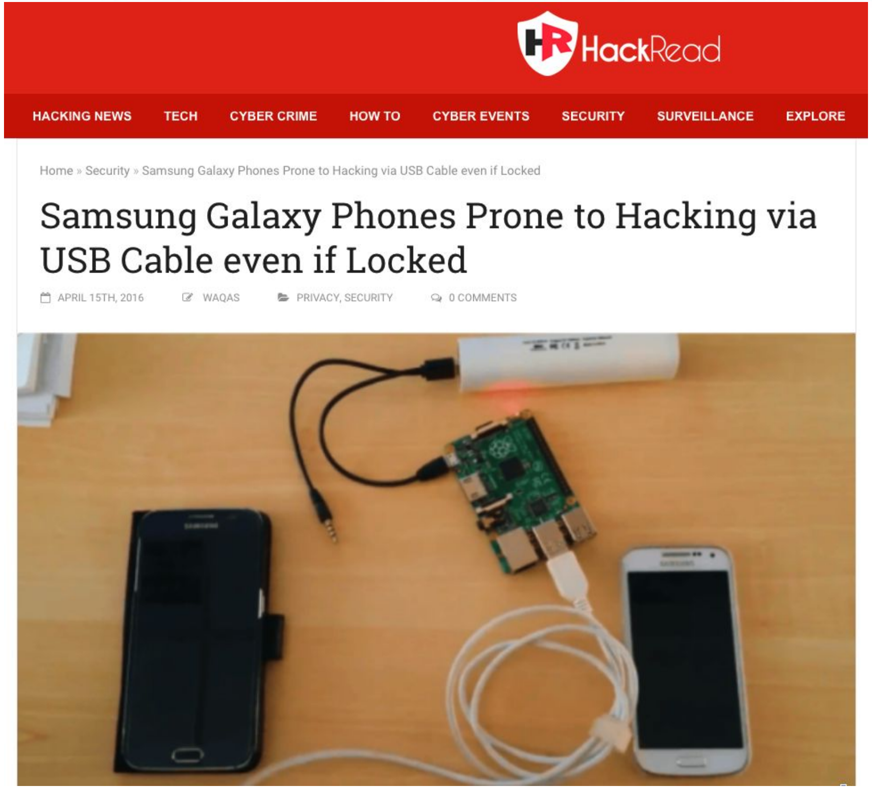
By Rafia Shaikh

May 27, 2016

26 SHARES

No, seriously - don't do this too...

# … And the hackers strike back

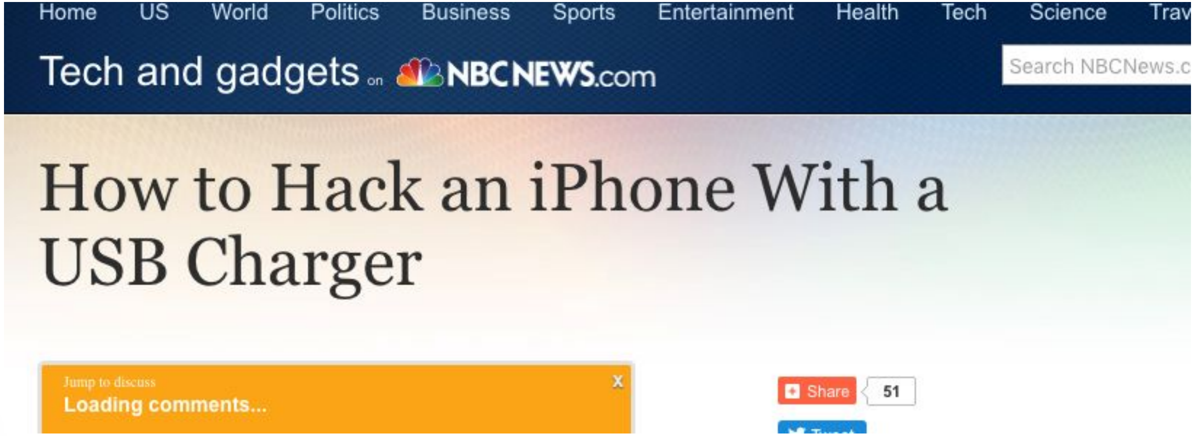


Home » Security » Samsung Galaxy Phones Prone to Hacking via USB Cable even if Locked

Samsung Galaxy Phones Prone to Hacking via USB Cable even if Locked

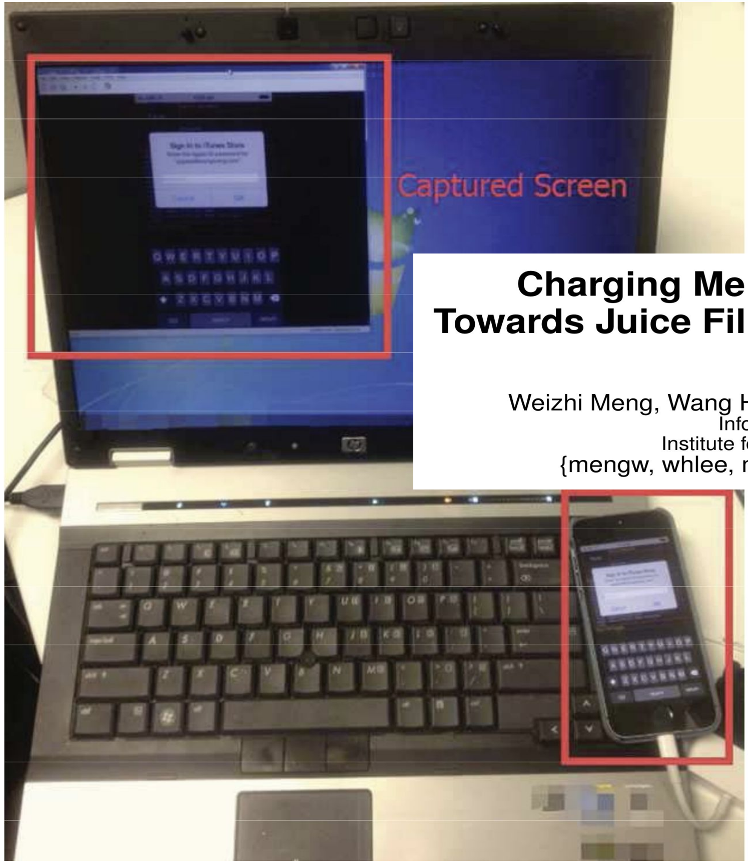
APRIL 15TH, 2016 WAQAS PRIVACY, SECURITY 0 COMMENTS

# … And the hackers strike back



How to Hack an iPhone With a USB Charger

# … And the hackers strike back

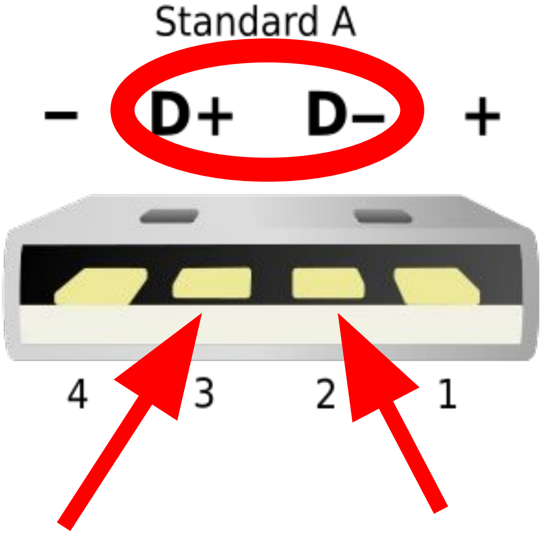


**Charging Me and I Know Your Secrets! Towards Juice Filming Attacks on Smartphones**

Weizhi Meng, Wang Hao Lee, S. R. Murali and S. P. T. Krishnan
Infocomm Security Department
Institute for Infocomm Research, Singapore
{mengw, whlee, muralism, krishnan}@i2r.a-star.edu.sg

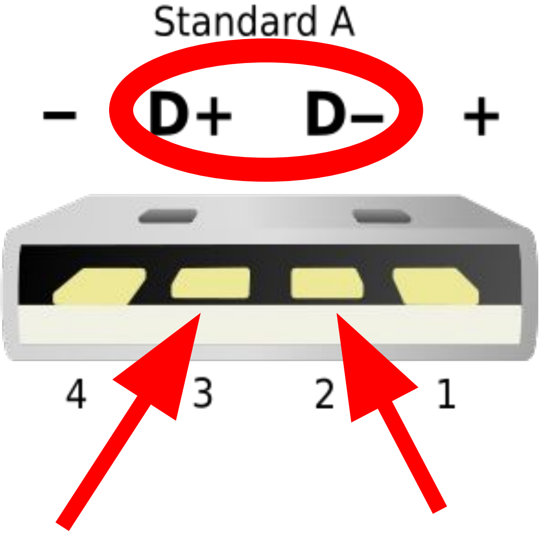
# The threat runs on the data cable

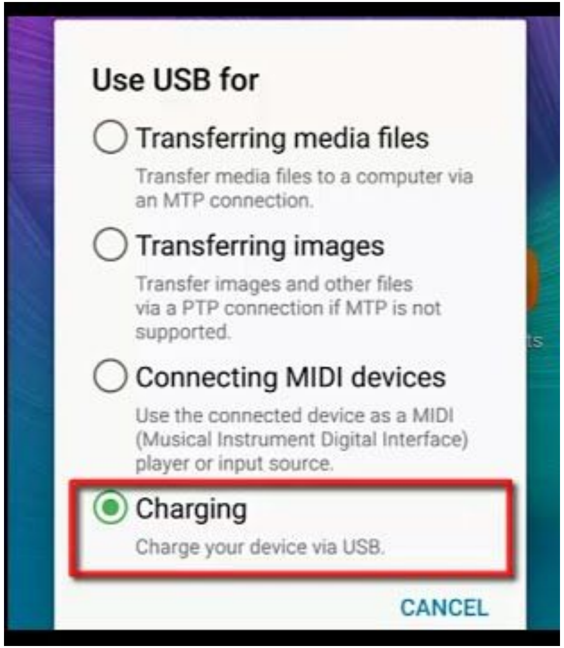
These attacks use the data transfer connection



# The threat runs on the data cable

These attacks use the data transfer connection





Use USB for

○ Transferring media files
Transfer media files to a computer via an MTP connection.

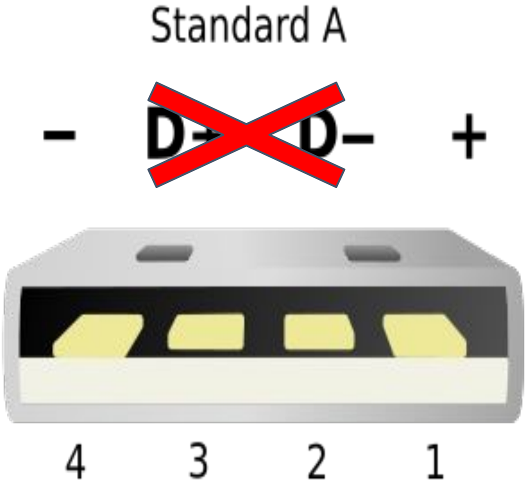
○ Transferring images
Transfer images and other files via a PTP connection if MTP is not supported.

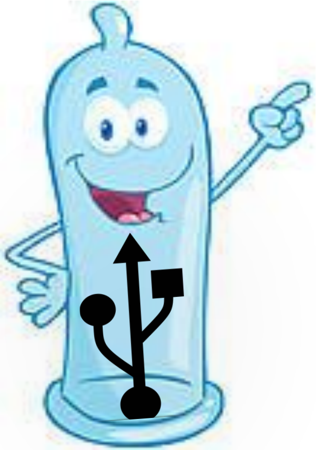
○ Connecting MIDI devices
Use the connected device as a MIDI (Musical Instrument Digital Interface) player or input source.

● Charging
Charge your device via USB.

# The threat runs on the data cable

Prevent unwanted surprises





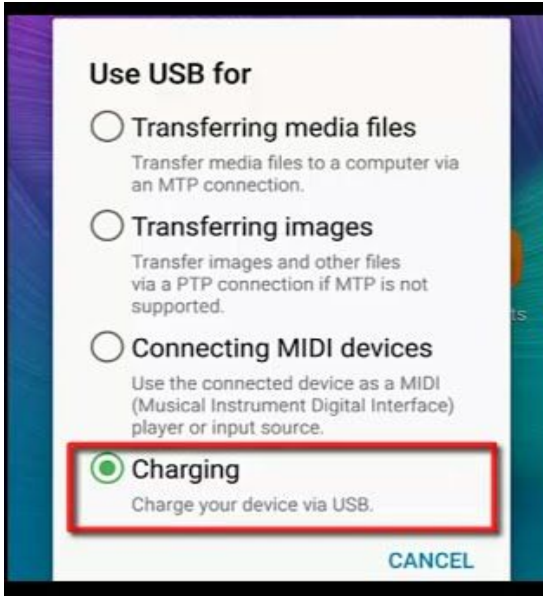
A.k.a
USB Condom

kenable Power Only USB Charging Cable Extension Lead 20cm
by kenable
★★★☆☆ 16 customer reviews

PortaPow PPSCA01 3rd Gen Data Blocker
by PortaPow
★★★★☆ 147 customer reviews | 10 answered questions
Amazon's Choice for "usb data blocker"

# The threat runs on the data cable

Are these precautions enough to prevent data getting stolen from our devices?



Use USB for

○ Transferring media files
Transfer media files to a computer via an MTP connection.

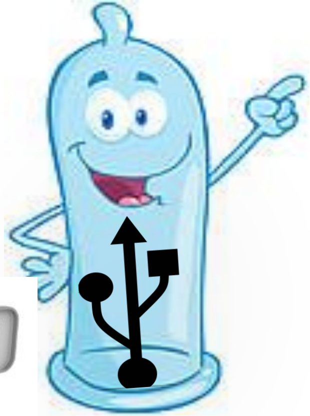
○ Transferring images
Transfer images and other files via a PTP connection if MTP is not supported.

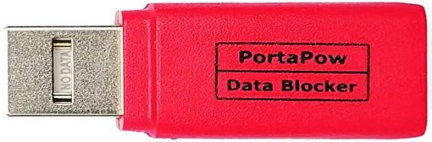
○ Connecting MIDI devices
Use the connected device as a MIDI (Musical Instrument Digital Interface) player or input source.

● Charging
Charge your device via USB.

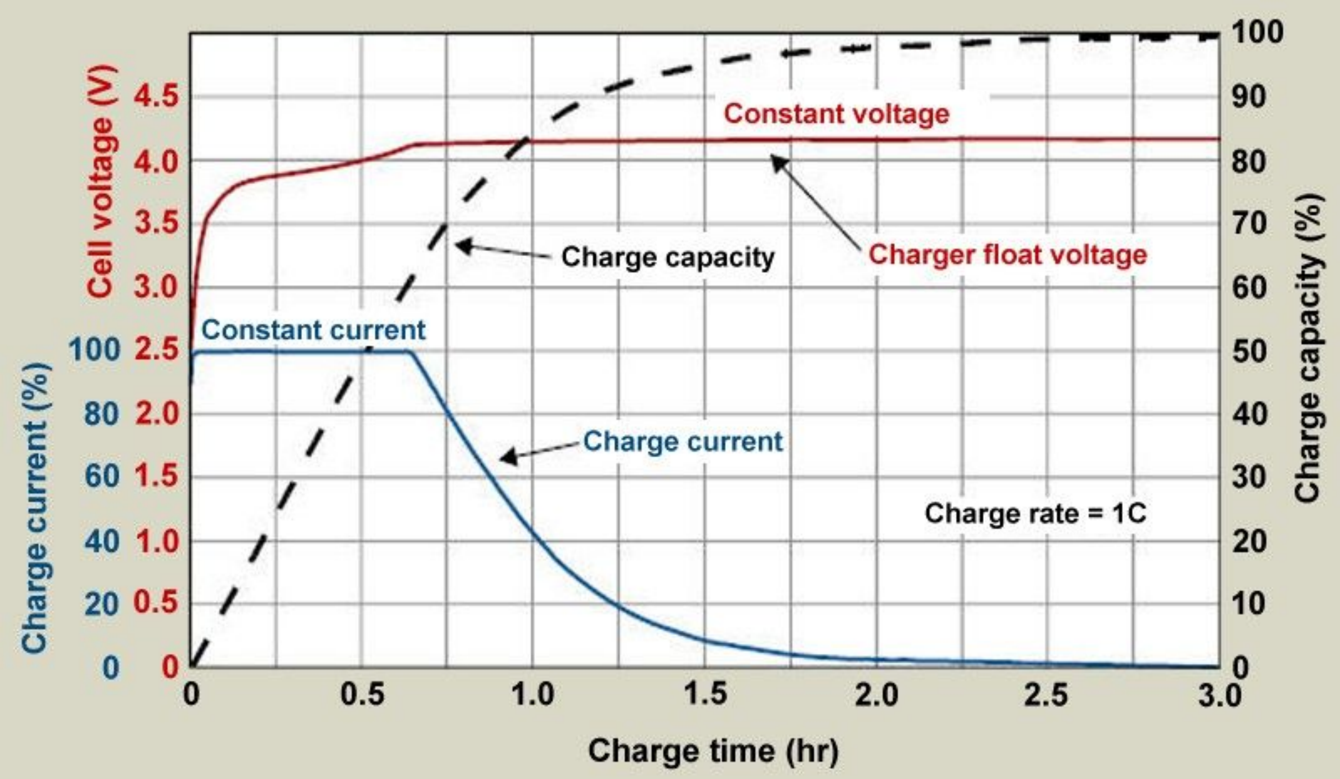
CANCEL

Well... **NO!**



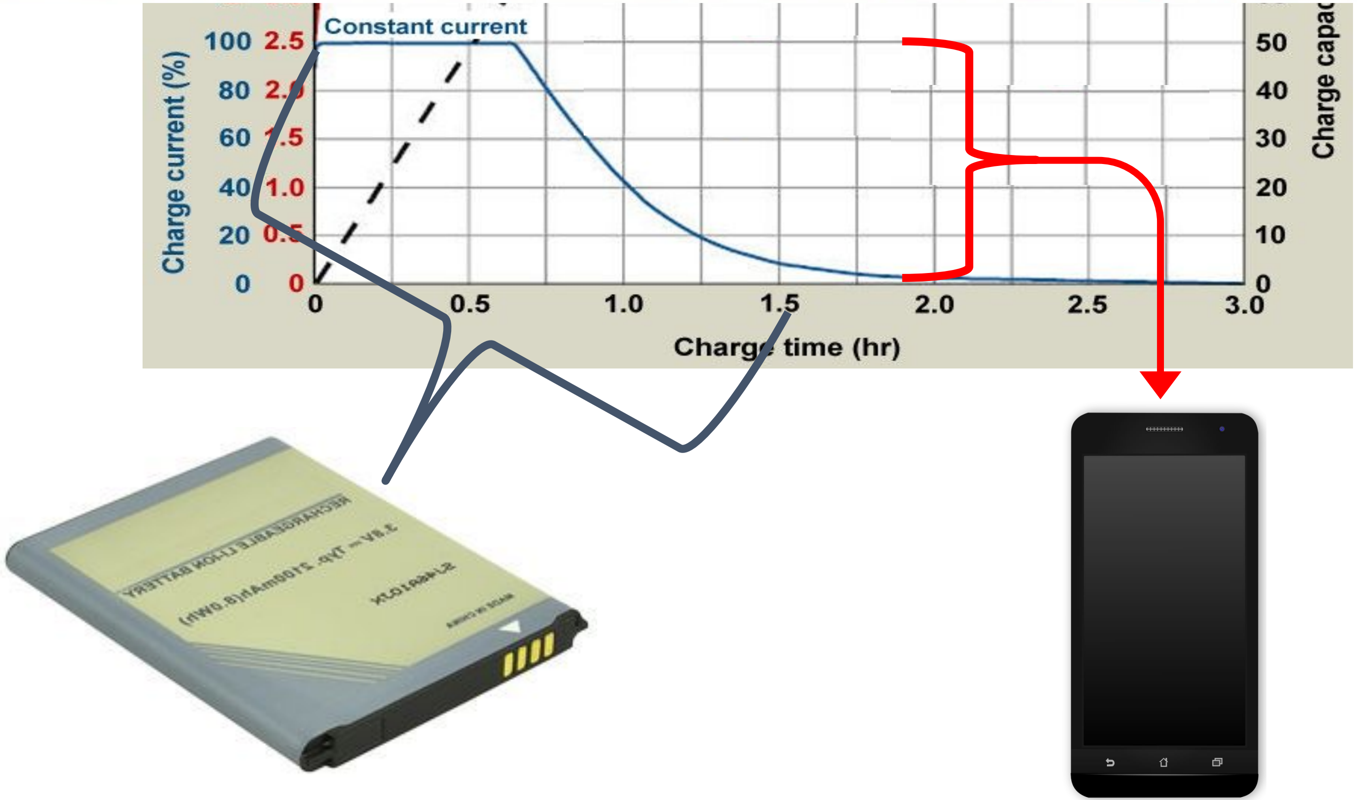


# Background: how a smartphone recharges?



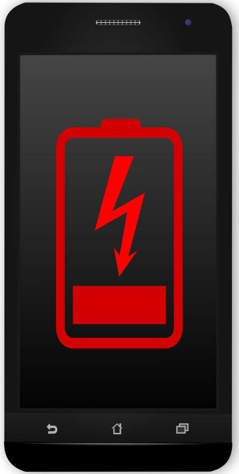
source: Cadex.com and Battery University
https://batteryuniversity.com/learn/article/charging_lithium_ion_batteries

# Background: where the current goes?



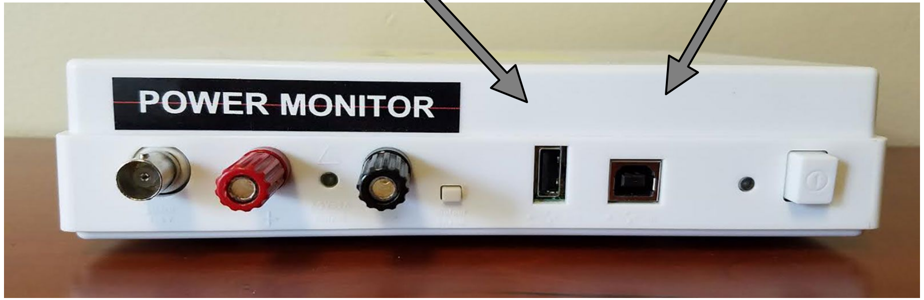
source: Cadex.com and Battery University
https://batteryuniversity.com/learn/article/charging_lithium_ion_batteries

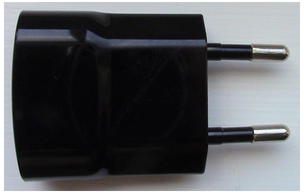
# Background: Let’s check this out!



Phone - USB Cable

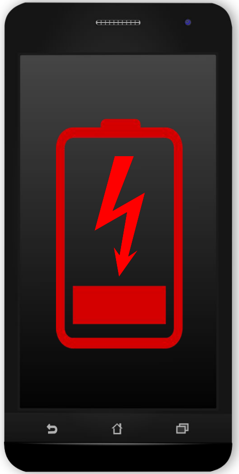
USB Cable - Power Source

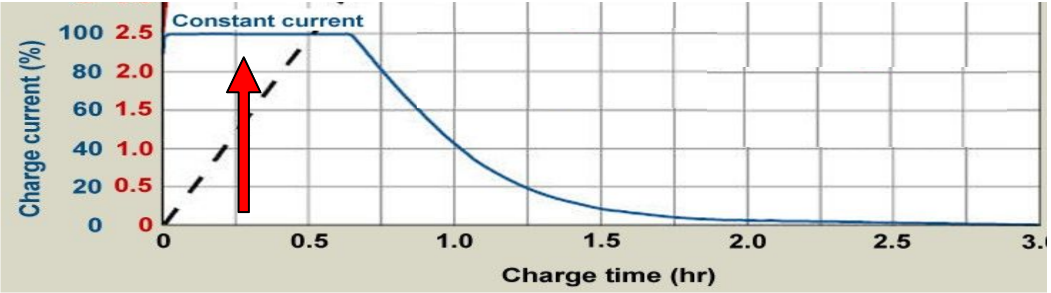


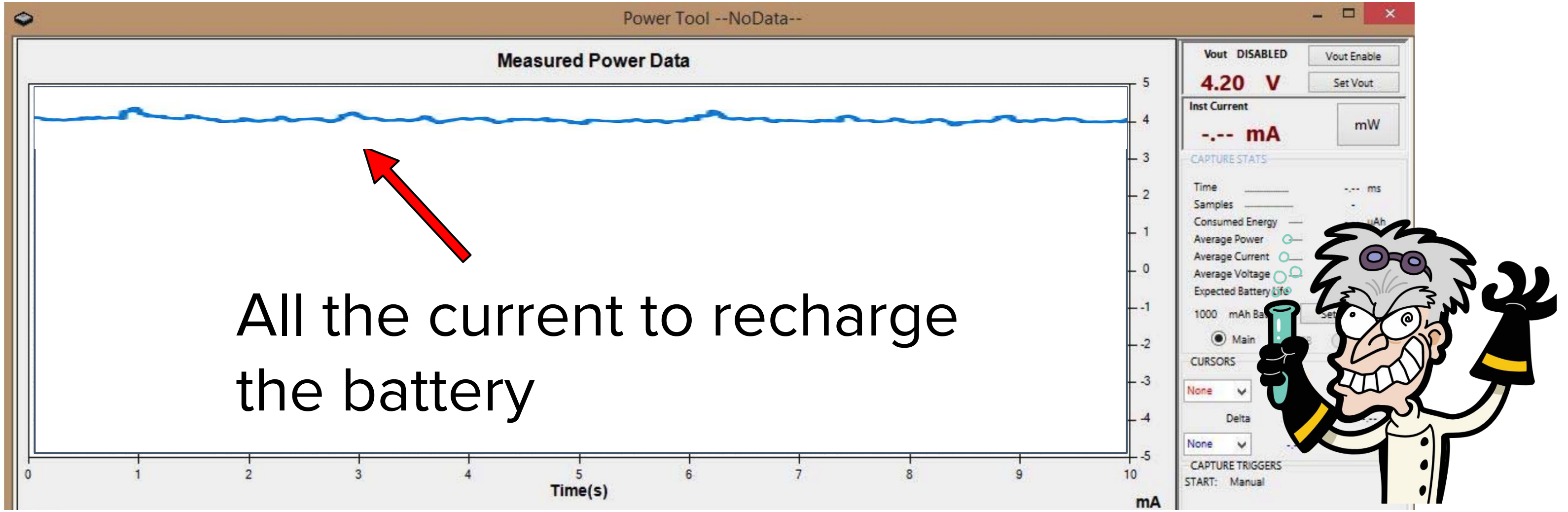


The Monsoon Solutions - https://www.msoon.com/

# Background: Let’s check this out!







Vout DISABLED

4.20 V

Inst Current

-.-- mA

Time -.-- ms

Samples -

Consumed Energy

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

● Main

None

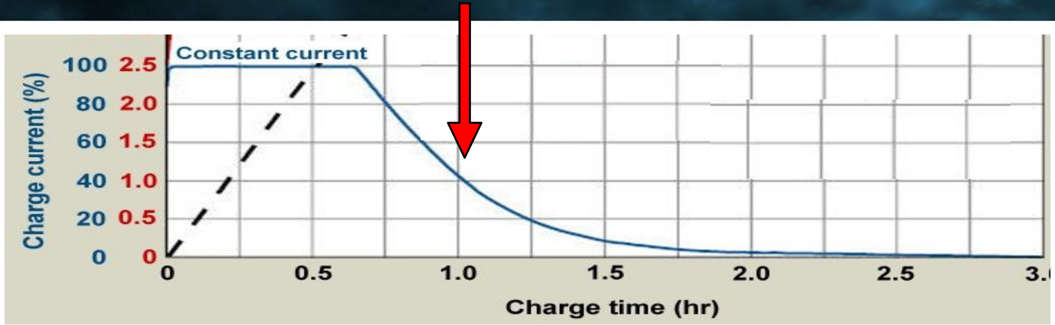
None

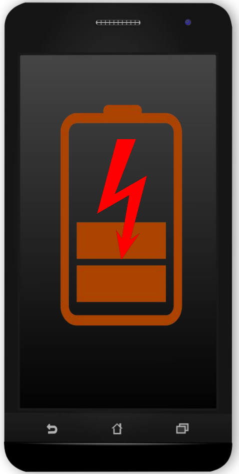
START: Manual

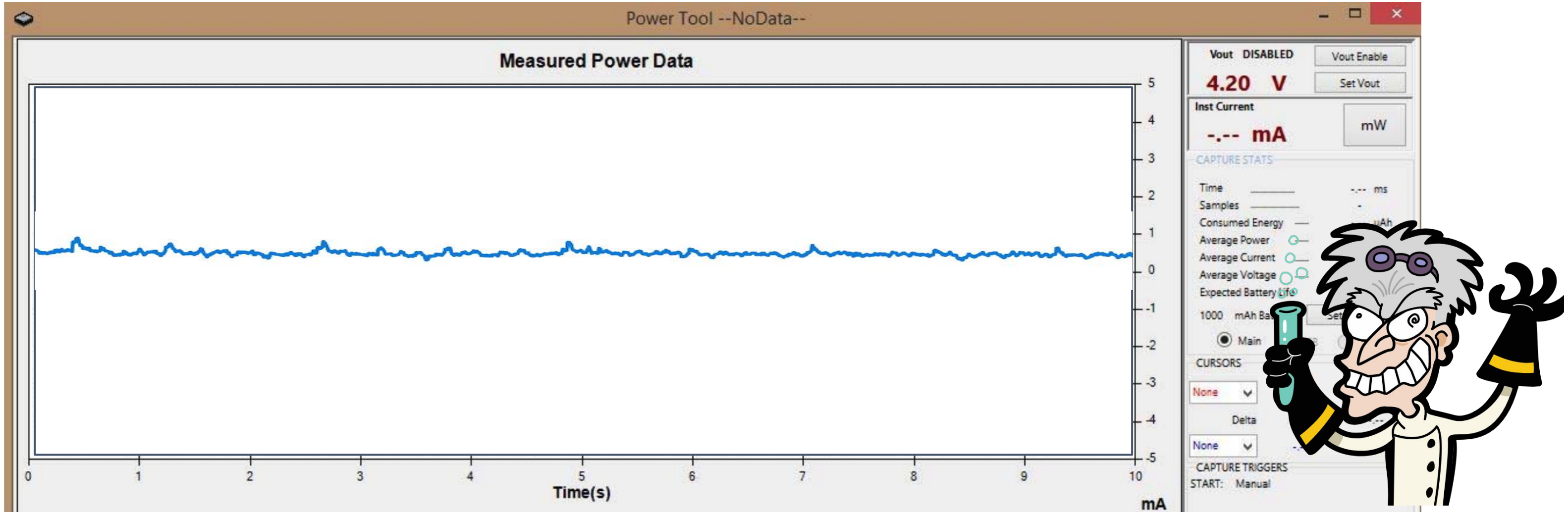
All the current to recharge the battery

The Monsoon Solutions - https://www.msoon.com/

# Background: Let's check this out!







Power Tool --NoData--

Measured Power Data

Vout DISABLED

4.20 V

Inst Current

-.-- mA

CAPTURE STATS

Time -.-- ms

Samples -

Consumed Energy uAh

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

Main

CURSORS

None

Delta

None

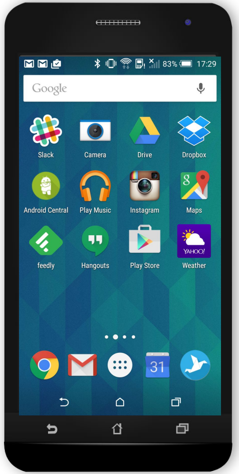
CAPTURE TRIGGERS

START: Manual

The Monsoon Solutions - https://www.msoon.com/

# Background: Let’s check this out!

## Display

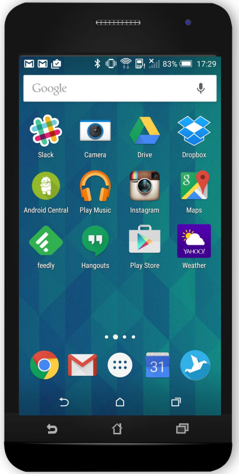


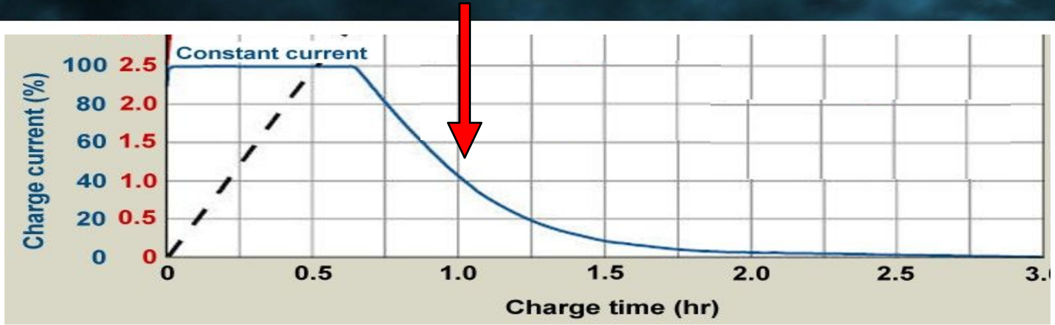
Let’s try to turn the display **on** and **off** and see what happens

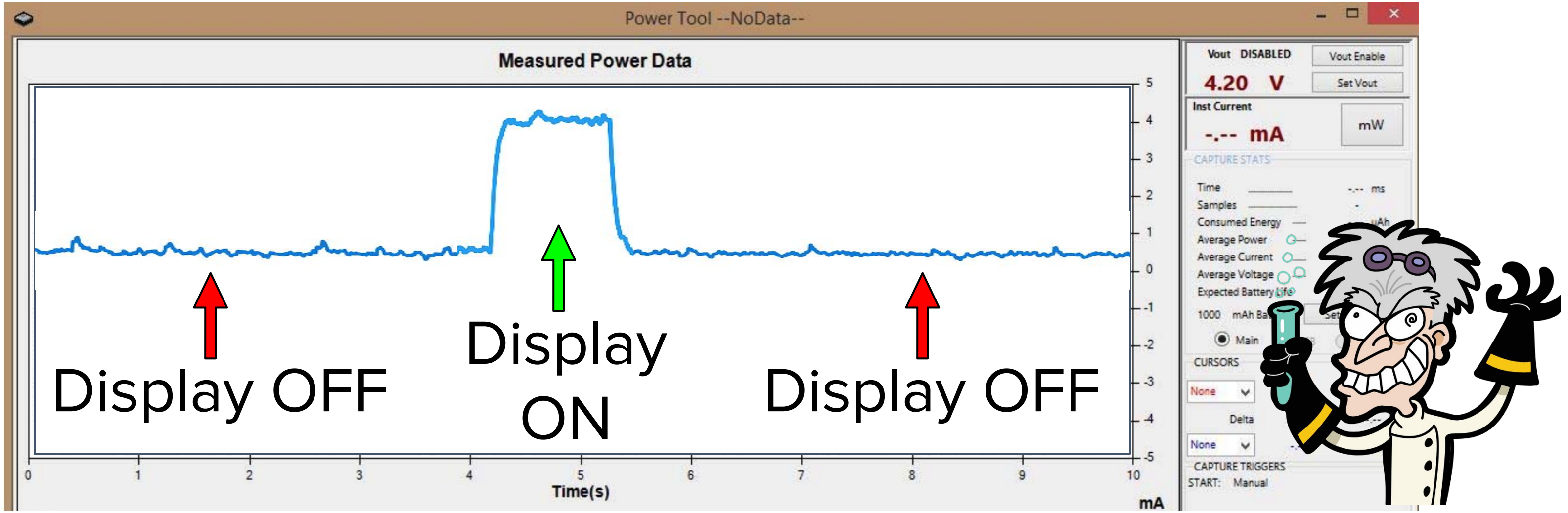
The Monsoon Solutions - https://www.msoon.com/

# Background: Let’s check this out!

## Display







Vout DISABLED

4.20 V

Inst Current

-.-- mA

Time -.-- ms

Samples -

Consumed Energy

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

None

None

START: Manual

Display OFF

Display ON

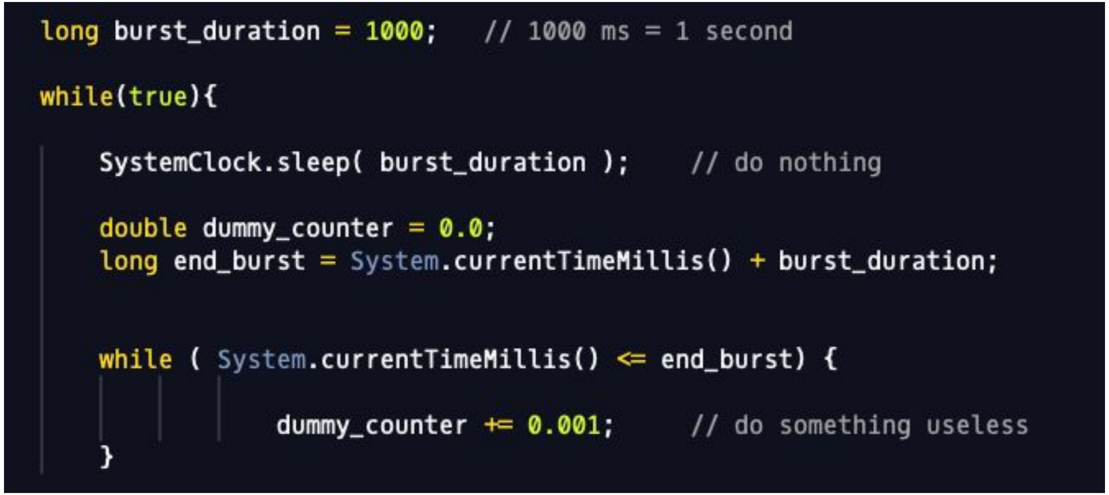
Display OFF

The Monsoon Solutions - https://www.msoon.com/

# Background: Let’s check this out!

## CPU bursts

And what about CPU bursts?

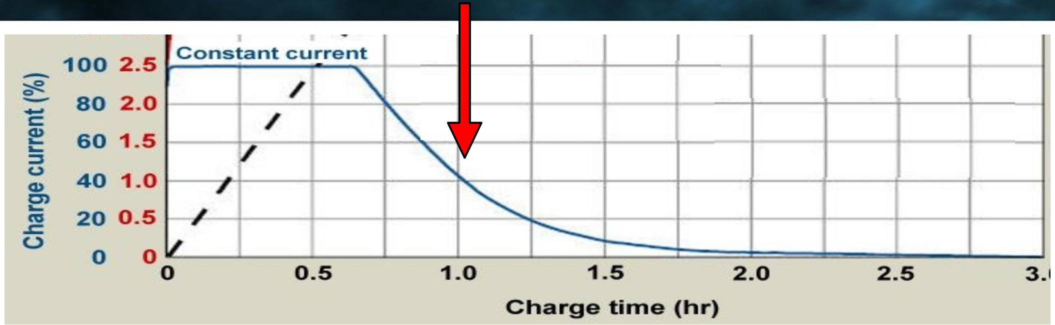


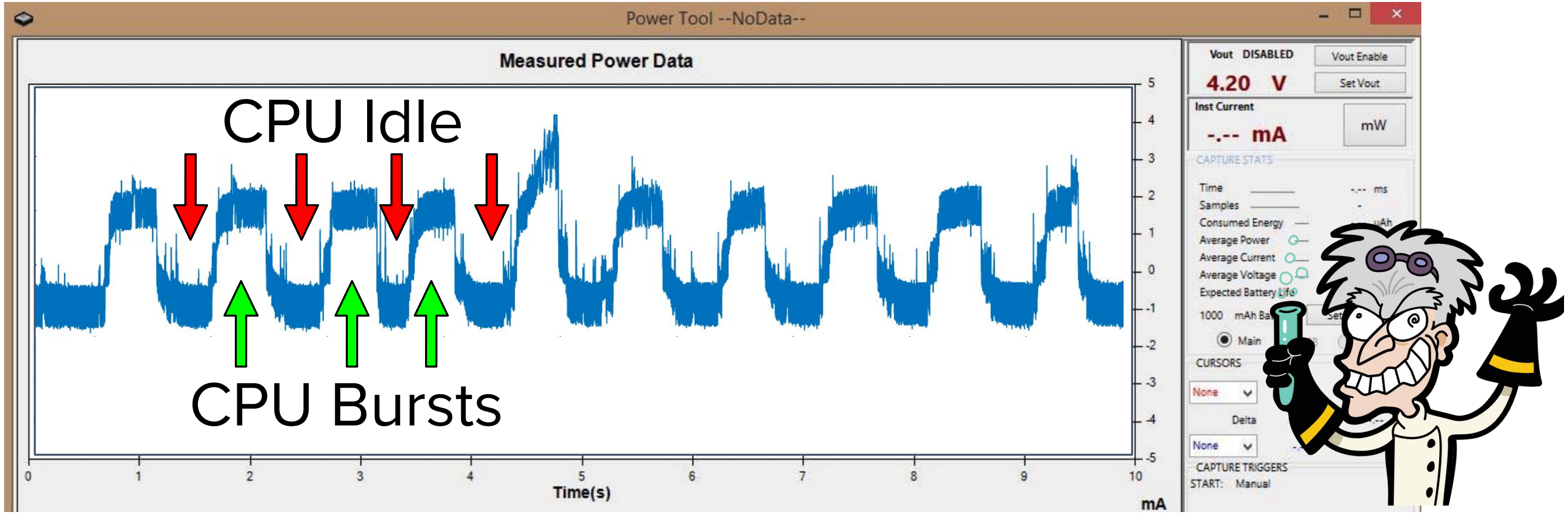
```
long burst_duration = 1000;    // 1000 ms = 1 second

while(true){

    SystemClock.sleep( burst_duration );    // do nothing

    double dummy_counter = 0.0;
    long end_burst = System.currentTimeMillis() + burst_duration;


    while ( System.currentTimeMillis() <= end_burst) {

                dummy_counter += 0.001;      // do something useless
    }
```

The Monsoon Solutions - https://www.msoon.com/

# Background: Let's check this out!

CPU bursts





CPU Idle

CPU Bursts

Vout DISABLED

4.20 V

Vout Enable

Set Vout

Inst Current

-.-- mA

mW

CAPTURE STATS

Time -.-- ms

Samples -

Consumed Energy

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

● Main

CURSORS

None

Delta

None

CAPTURE TRIGGERS

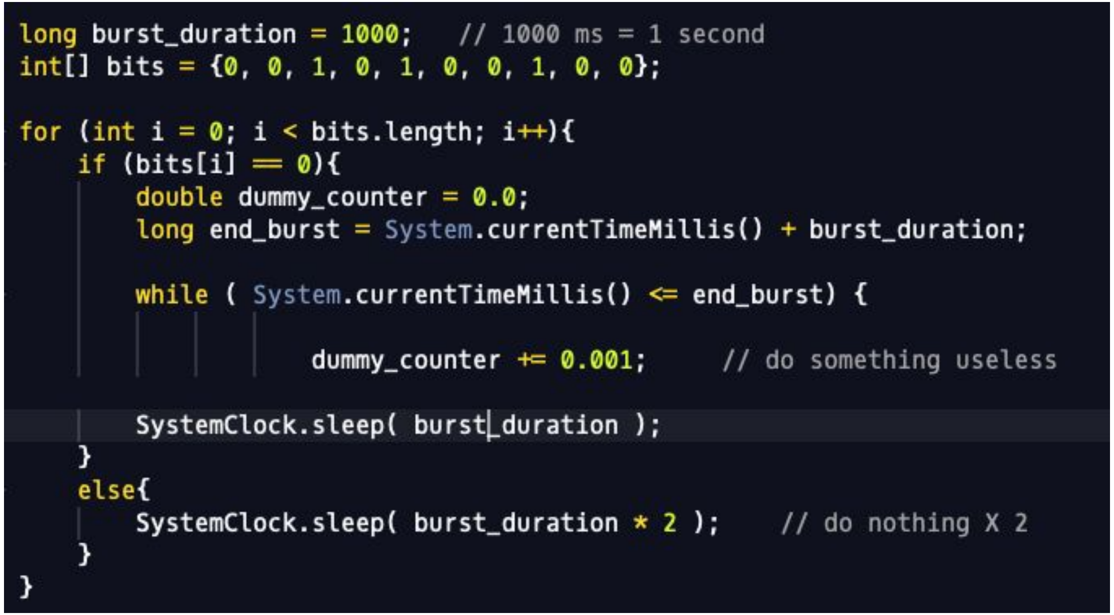
START: Manual

The Monsoon Solutions - https://www.msoon.com/

# A little step forward...

CPU bursts

- 0 → Burst
- 1 → Nothing

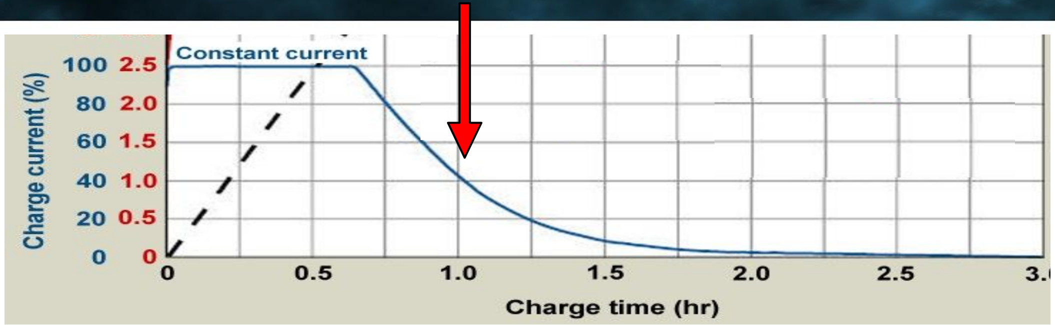


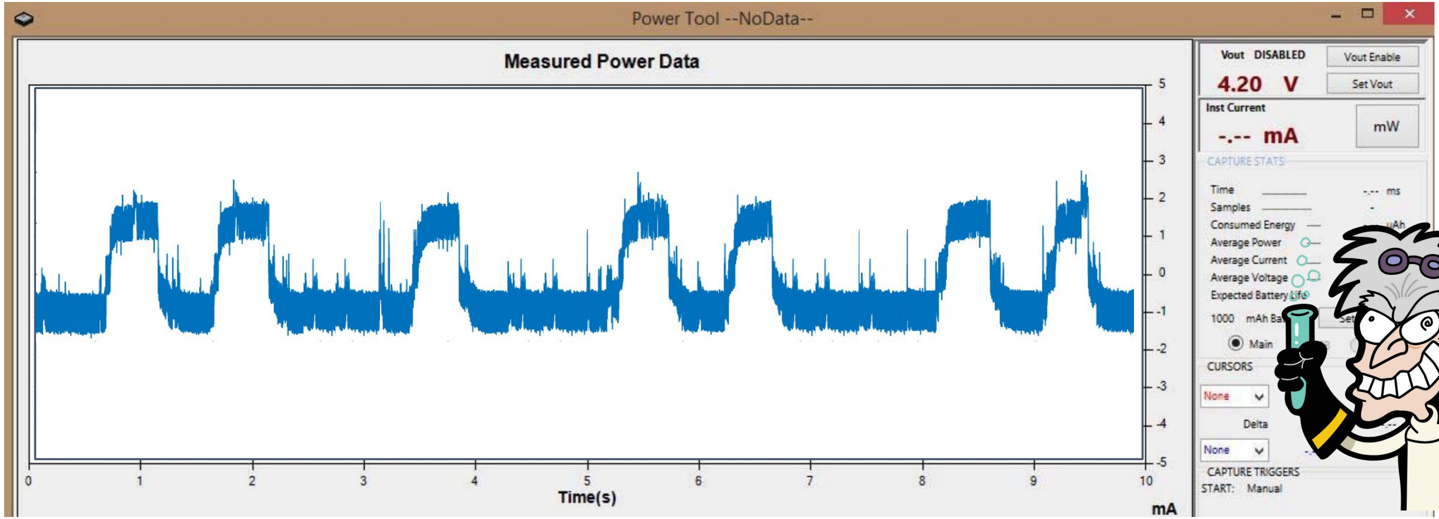
```
long burst_duration = 1000;   // 1000 ms = 1 second
int[] bits = {0, 0, 1, 0, 1, 0, 0, 1, 0, 0};

for (int i = 0; i < bits.length; i++){
    if (bits[i] == 0){
        double dummy_counter = 0.0;
        long end_burst = System.currentTimeMillis() + burst_duration;

        while ( System.currentTimeMillis() <= end_burst) {

                    dummy_counter += 0.001;     // do something useless

        SystemClock.sleep( burst_duration );
    }
    else{
        SystemClock.sleep( burst_duration * 2 );    // do nothing X 2
    }
}
```

The Monsoon Solutions - https://www.msoon.com/

# We have a covert channel

CPU bursts





Power Tool --NoData--

Vout DISABLED

4.20 V

Vout Enable

Set Vout

Inst Current

-.-- mA

mW

CAPTURE STATS

Time -.-- ms

Samples

Consumed Energy

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

● Main

CURSORS

None

Delta

None

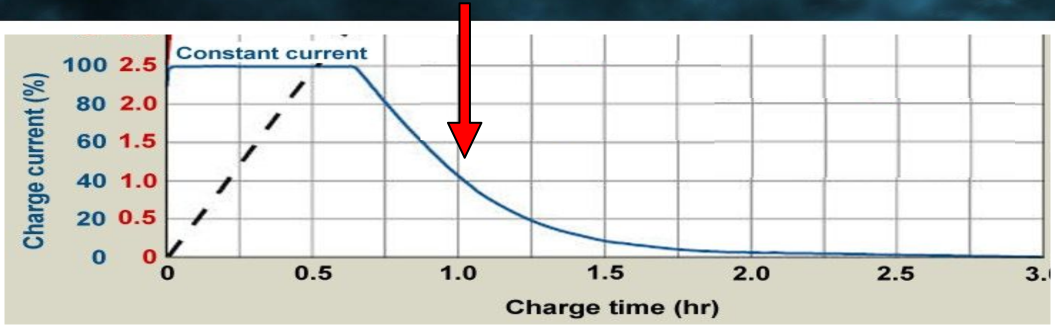
CAPTURE TRIGGERS

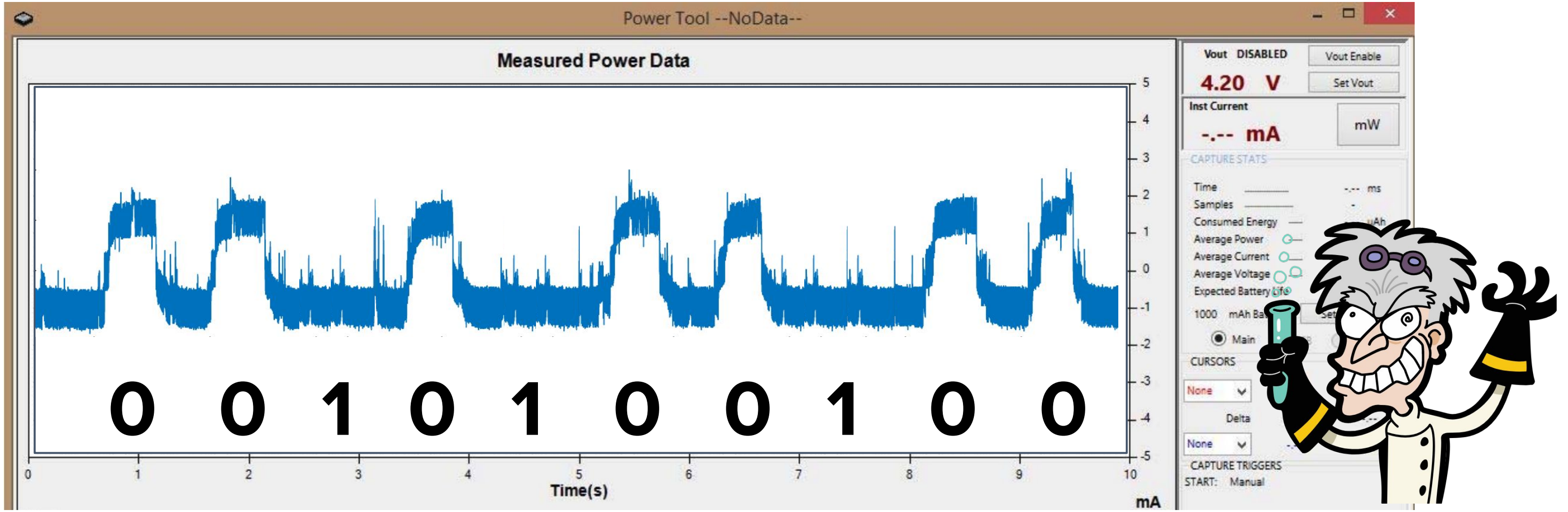
START: Manual

The Monsoon Solutions - https://www.msoon.com/

# We have a covert channel

CPU bursts





0 0 1 0 1 0 0 1 0 0

Vout DISABLED

4.20 V

Inst Current

-.-- mA

Time -.-- ms

Samples -

Consumed Energy uAh

Average Power

Average Current

Average Voltage

Expected Battery Life

1000 mAh Ba

● Main

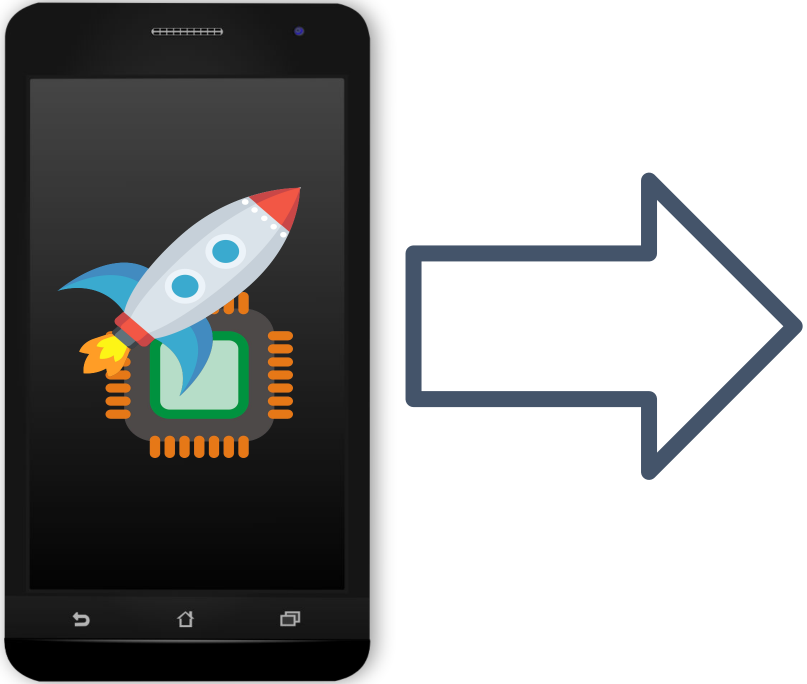
None

None

START: Manual

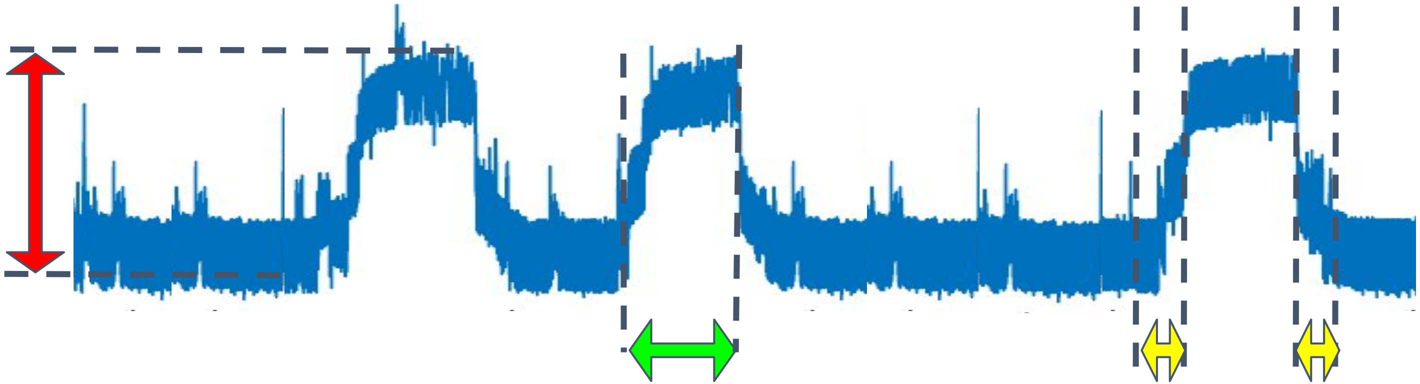
The Monsoon Solutions - https://www.msoon.com/

# We have found a covert channel



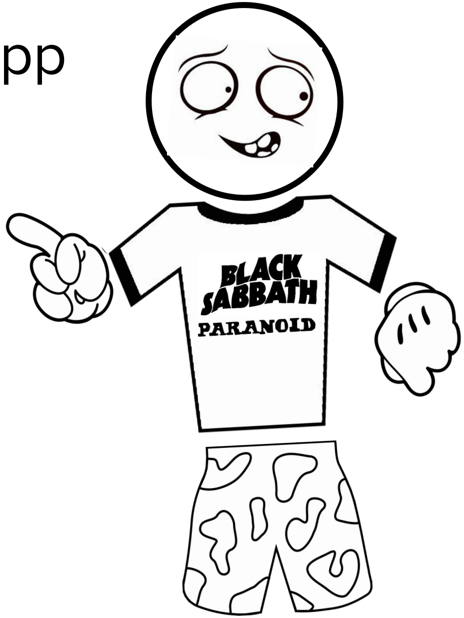
# Properties of the covert channel

- We cannot control the amplitude ↕ of bursts…
- … But we can control the timing ↔
- Transition time idle/burst ↔ is not instantaneous



# Let me present Bob

- Bob has a secret info **X** on his smartphone
- Bob does **not** allow his apps to access to the **Internet**
- Bob double-checks the **permissions** given to each app
- Bob always uses the **USB condom**
- Because he knows about the **security risks** of using free charging stations
- Bob cares about his **privacy**
- (Be like Bob)

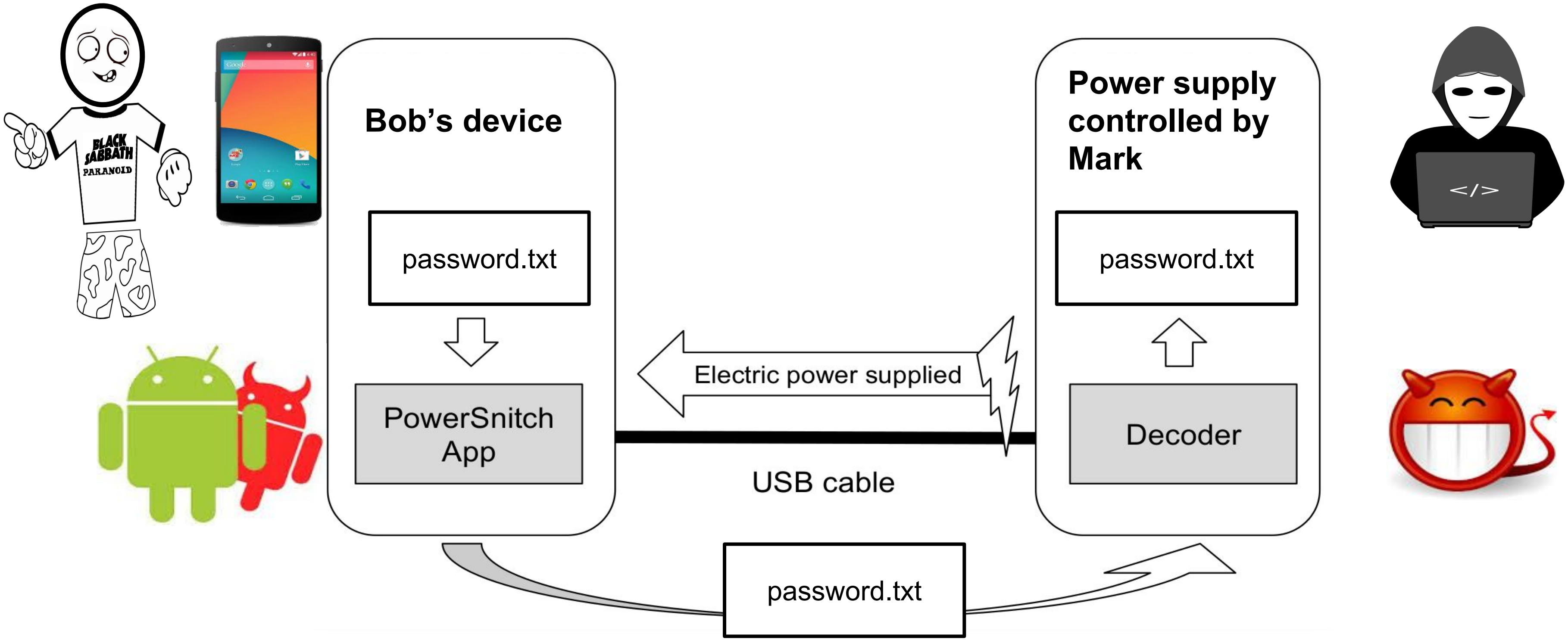


# And here is Mark, the hacker

- Mark knows that Bob has a secret **X** on his smartphone
- Mark was able to **install an app** on Bob’s smartphone
- The app cannot use any network connection
- Mark is highly motivated to steal **X** from Bob

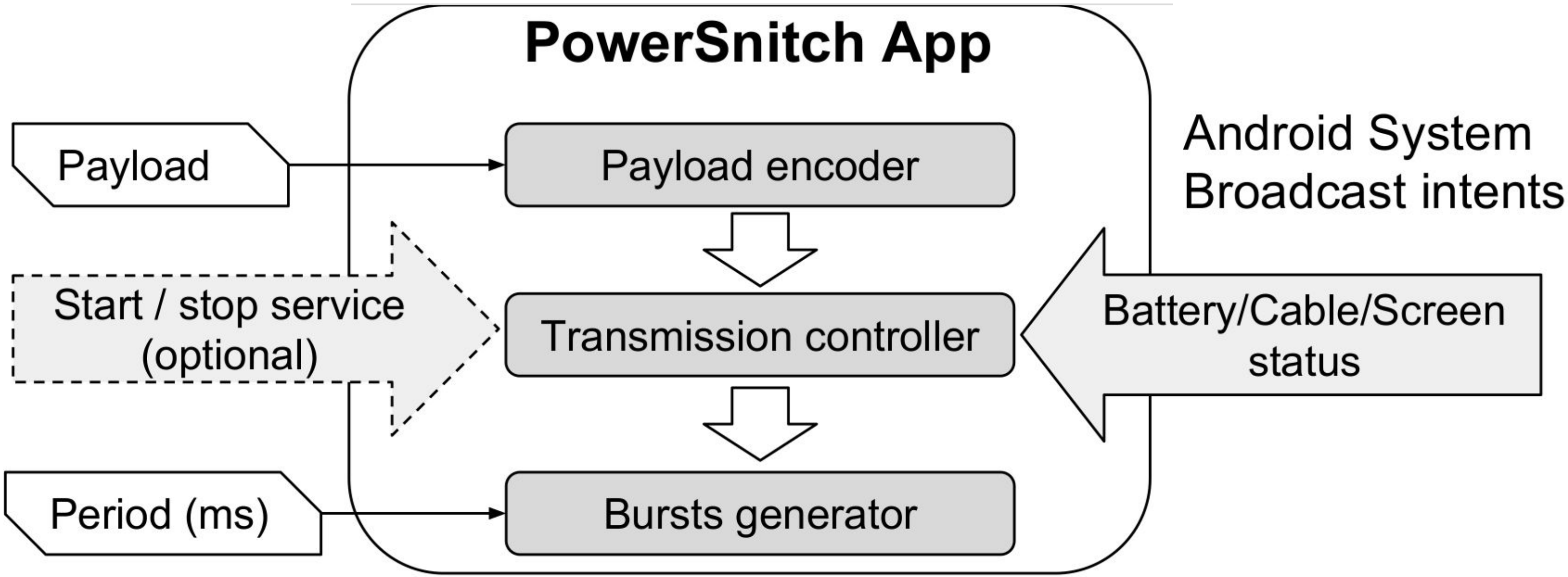
How can Mark exfiltrate **X** from Bob’s smartphone?

# How can Mark exploit this covert channel?

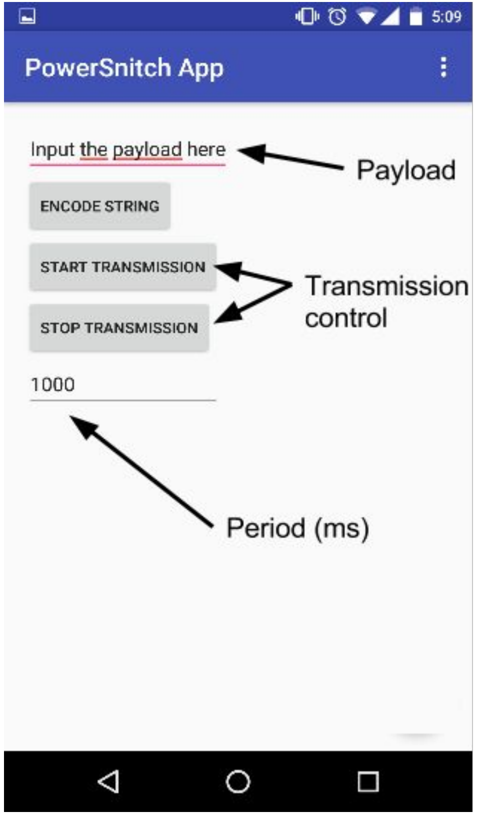


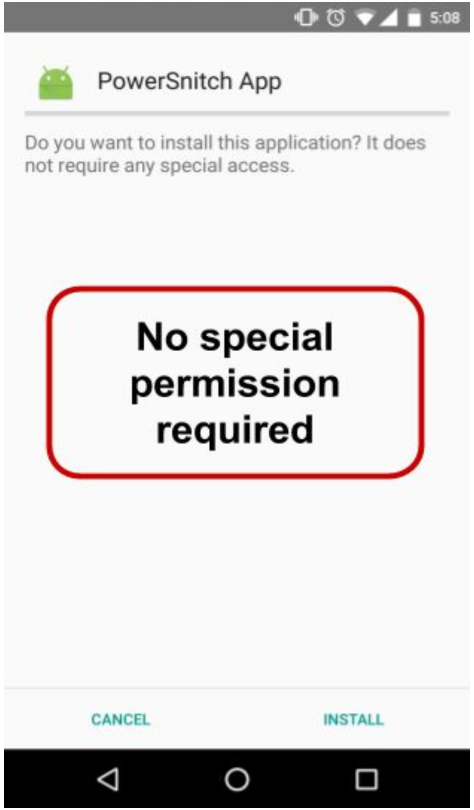
Riccardo Spolaor, Laila Abudahi, Veelasha Moonsamy, Mauro Conti, and Radha Poovendran
"No Free Charge Theorem: A Covert Channel via USB Charging Cable on Mobile Devices" in ACNS 2017

# PowerSnitch app: our prototype



# PowerSnitch app: our prototype





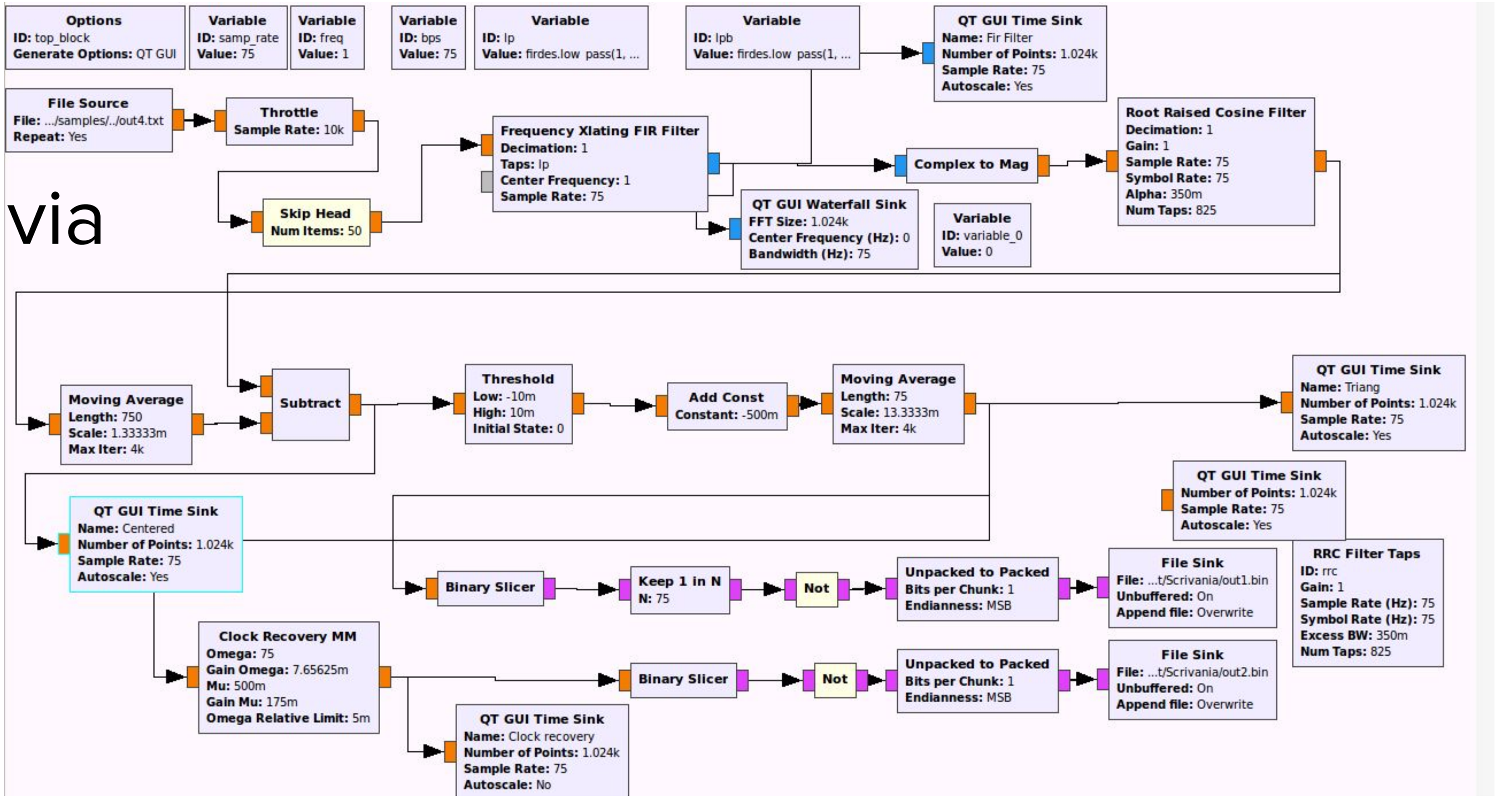
Do you want to install this application? It does not require any special access.

No special permission required

- It does **not** use Internet access
- It only needs the **permission** to access the **info to exfiltrate**

# Decoder: from the signal to the information

Signal processing via GNURadio



**Options**
**ID:** top_block
**Generate Options:** QT GUI

**Variable**
**ID:** samp_rate
**Value:** 75

**Variable**
**ID:** freq
**Value:** 1

**Variable**
**ID:** bps
**Value:** 75

**Variable**
**ID:** lp
**Value:** firdes.low_pass(1, ...

**Variable**
**ID:** lpb
**Value:** firdes.low_pass(1, ...

**QT GUI Time Sink**
**Name:** Fir Filter
**Number of Points:** 1.024k
**Sample Rate:** 75
**Autoscale:** Yes

**File Source**
**File:** .../samples/../out4.txt
**Repeat:** Yes

**Throttle**
**Sample Rate:** 10k

**Frequency Xlating FIR Filter**
**Decimation:** 1
**Taps:** lp
**Center Frequency:** 1
**Sample Rate:** 75

**Complex to Mag**

**Root Raised Cosine Filter**
**Decimation:** 1
**Gain:** 1
**Sample Rate:** 75
**Symbol Rate:** 75
**Alpha:** 350m
**Num Taps:** 825

**Skip Head**
**Num Items:** 50

**QT GUI Waterfall Sink**
**FFT Size:** 1.024k
**Center Frequency (Hz):** 0
**Bandwidth (Hz):** 75

**Variable**
**ID:** variable_0
**Value:** 0

**Moving Average**
**Length:** 750
**Scale:** 1.33333m
**Max Iter:** 4k

**Subtract**

**Threshold**
**Low:** -10m
**High:** 10m
**Initial State:** 0

**Add Const**
**Constant:** -500m

**Moving Average**
**Length:** 75
**Scale:** 13.3333m
**Max Iter:** 4k

**QT GUI Time Sink**
**Name:** Triang
**Number of Points:** 1.024k
**Sample Rate:** 75
**Autoscale:** Yes

**QT GUI Time Sink**
**Number of Points:** 1.024k
**Sample Rate:** 75
**Autoscale:** Yes

**QT GUI Time Sink**
**Name:** Centered
**Number of Points:** 1.024k
**Sample Rate:** 75
**Autoscale:** Yes

**Binary Slicer**

**Keep 1 in N**
**N:** 75

**Not**

**Unpacked to Packed**
**Bits per Chunk:** 1
**Endianness:** MSB

**File Sink**
**File:** ...t/Scrivania/out1.bin
**Unbuffered:** On
**Append file:** Overwrite

**RRC Filter Taps**
**ID:** rrc
**Gain:** 1
**Sample Rate (Hz):** 75
**Symbol Rate (Hz):** 75
**Excess BW:** 350m
**Num Taps:** 825

**Clock Recovery MM**
**Omega:** 75
**Gain Omega:** 7.65625m
**Mu:** 500m
**Gain Mu:** 175m
**Omega Relative Limit:** 5m

**Binary Slicer**

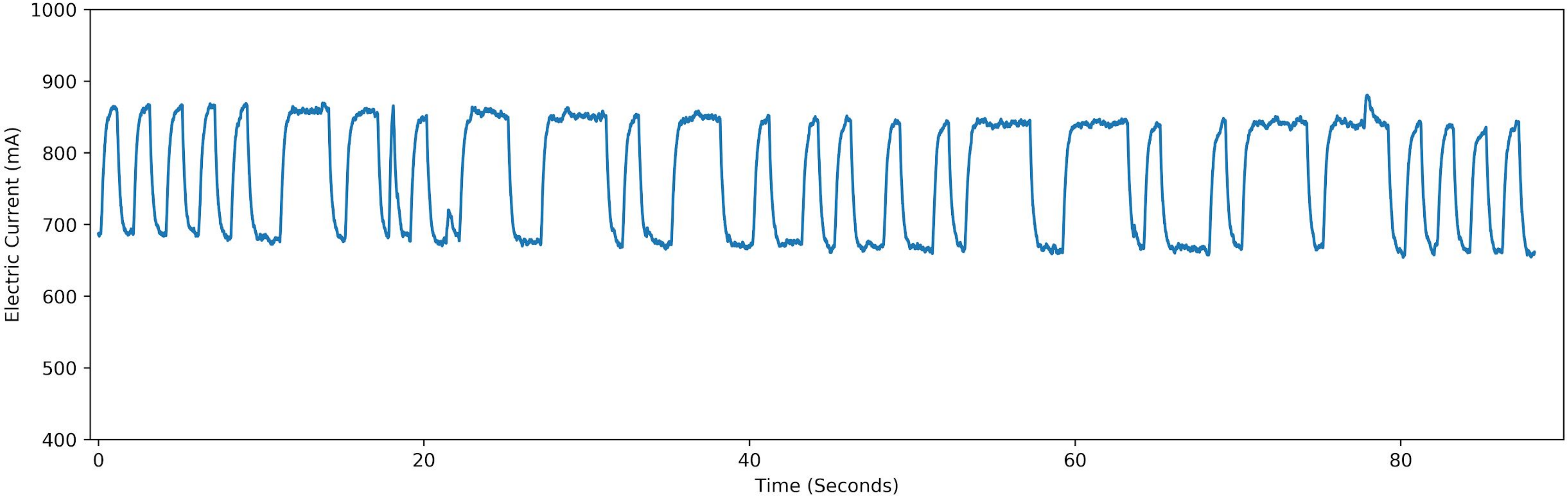
**Not**

**Unpacked to Packed**
**Bits per Chunk:** 1
**Endianness:** MSB

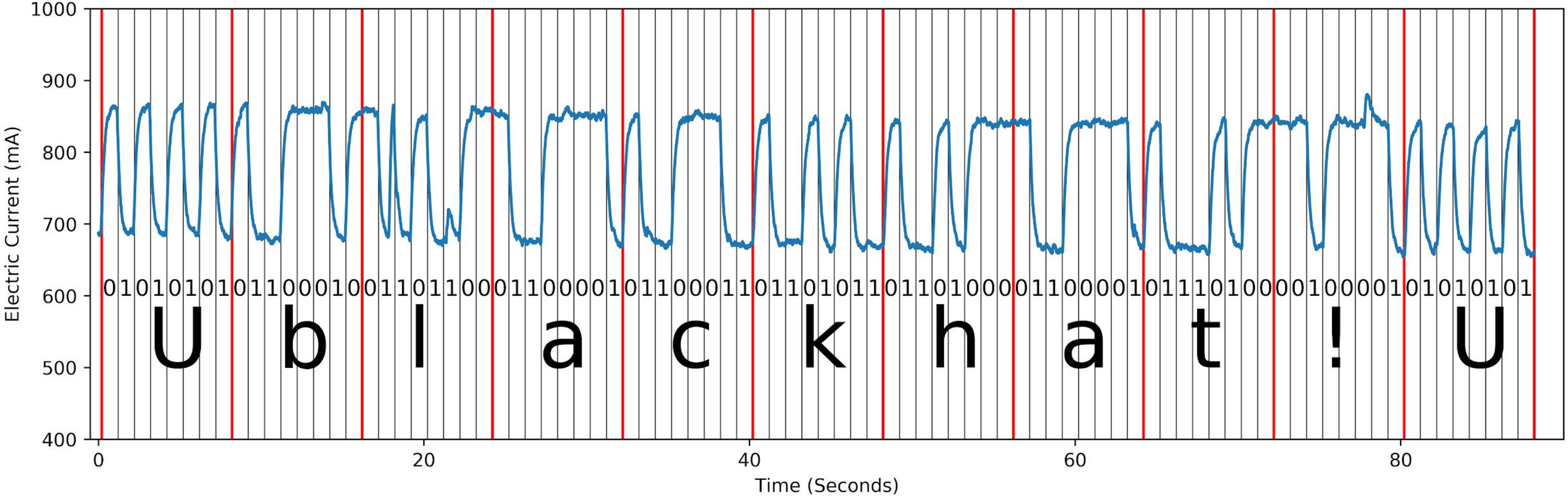
**File Sink**
**File:** ...t/Scrivania/out2.bin
**Unbuffered:** On
**Append file:** Overwrite

**QT GUI Time Sink**
**Name:** Clock recovery
**Number of Points:** 1.024k
**Sample Rate:** 75
**Autoscale:** No

# Decoder: from the signal to the information



# Decoder: from the signal to the information



# PowerSnitch app: Optimizations

# PowerSnitch app: Optimizations

# PowerSnitch app: Optimizations (1/2)

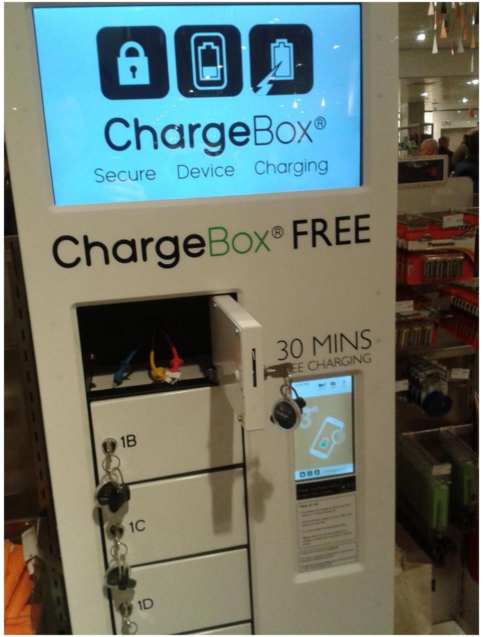
- It requires no special permission
- It does not require internet access at all
- Doze mode not active (battery saving)

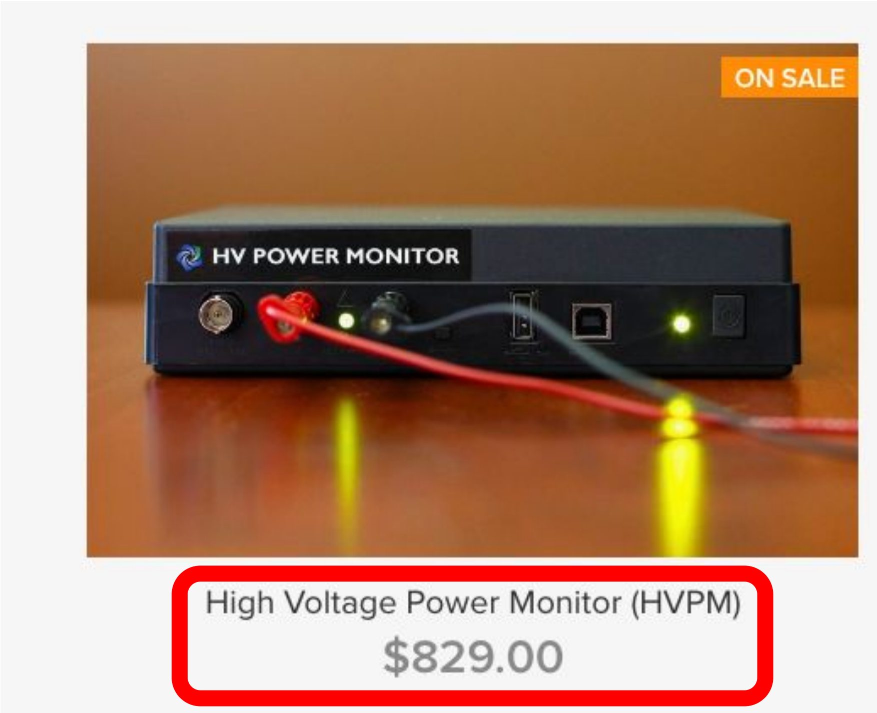
- App can be:
  - Apparently innocuous app (e.g., alarm clock)
  - A popular app repackaged

# PowerSnitch app: Optimizations (2/2)

- CPU bursts cannot be easily detected (a flashing screen, yes)
- Transmit only when:
  - The screen is off (smartphone is inactive)
  - ADB debugging mode not active
  - The battery is charged enough (>50%)
  - The power supply is listening
- It does not affect battery charging

# NFCT 1.0: First version of the attack





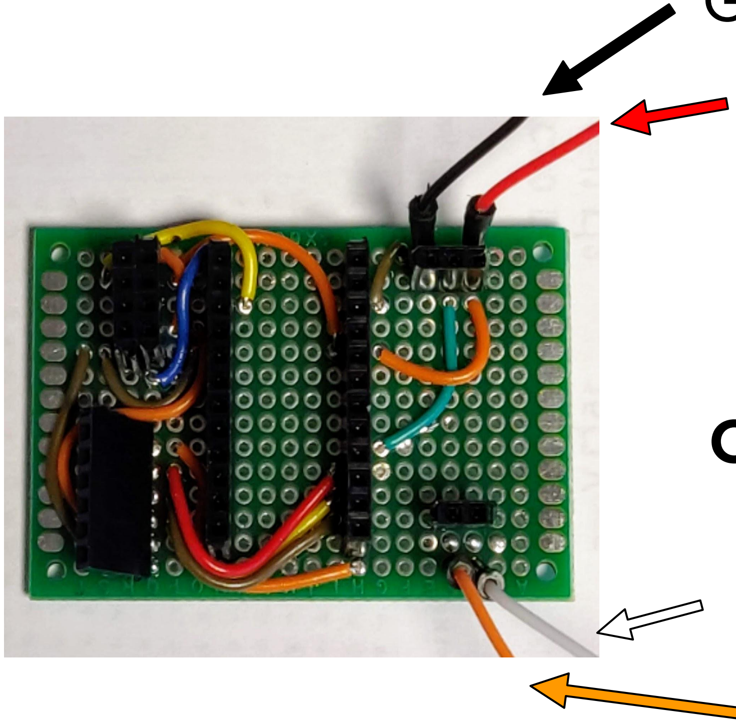
High Voltage Power Monitor (HVPM)

$829.00

# NFCT 2.0: new version of the attack

- Cheaper
- Smaller
- Easier to deploy

# Decoder: Electronics DIY



GND (-)

VCC (+5V)

**Current to measure**

Power supply’s side

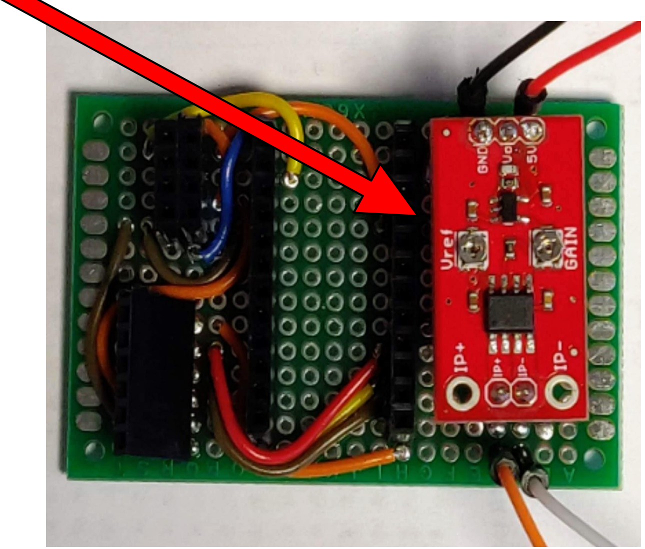
Smartphone’s side

# Decoder: Electronics DIY

Hall effect current sensor
(e.g., ACS712)

GND (-)

VCC (+5V)



**Current to measure**

Power supply's side

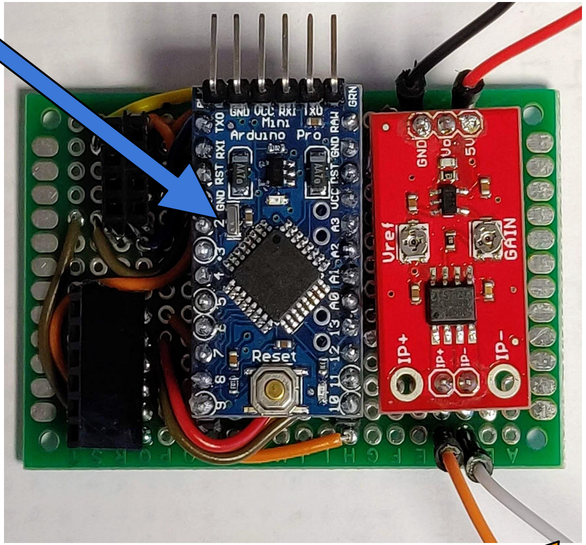
Smartphone's side

# Decoder: Electronics DIY

Arduino Mini PRO

GND (-)

VCC (+5V)



**Current to measure**

Power supply’s side

Smartphone’s side

black hat EUROPE 2018

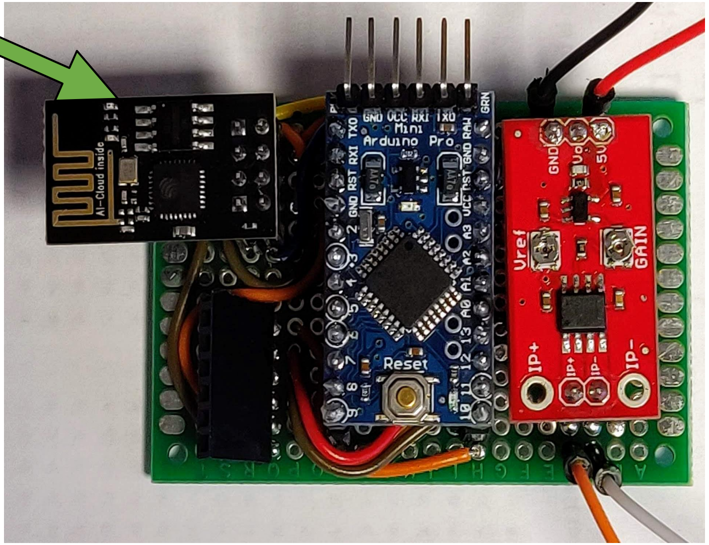
# Decoder: Electronics DIY

WiFI module

GSM module

GND (-)

VCC (+5V)



**Current to measure**

Power supply’s side

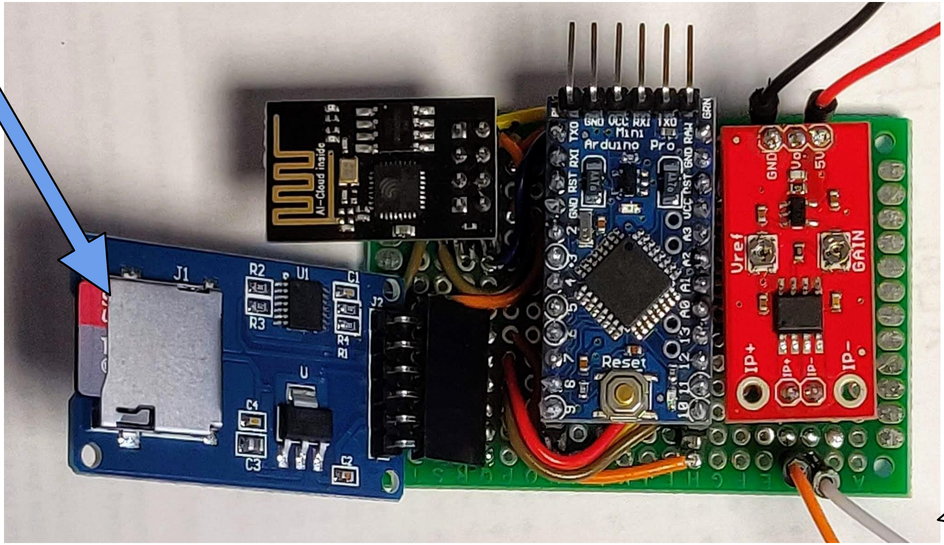
Smartphone’s side

# Decoder: Electronics DIY

MicroSD card Module

GND (-)

VCC (+5V)



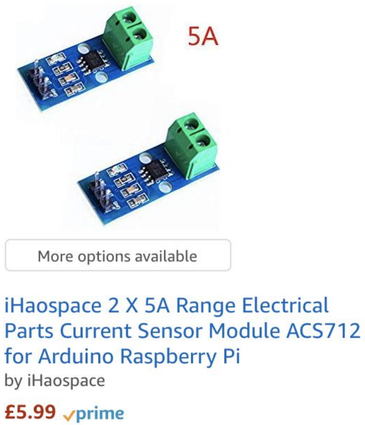
**Current to measure**

Power supply's side

Smartphone's side

# Decoder: Easy to deploy

# Electronics DIY: cost?

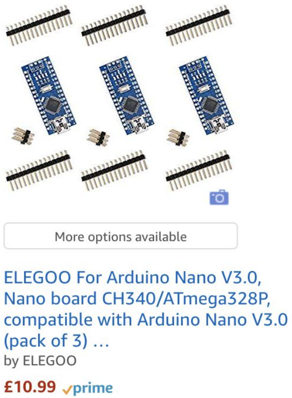

5A

More options available

iHaospace 2 X 5A Range Electrical Parts Current Sensor Module ACS712 for Arduino Raspberry Pi

by iHaospace

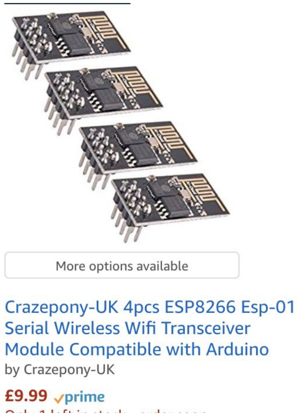
£5.99 prime


More options available

ELEGOO For Arduino Nano V3.0, Nano board CH340/ATmega328P, compatible with Arduino Nano V3.0 (pack of 3) …

by ELEGOO

£10.99 prime

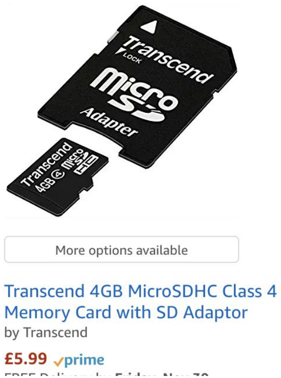

More options available

Crazepony-UK 4pcs ESP8266 Esp-01 Serial Wireless Wifi Transceiver Module Compatible with Arduino

by Crazepony-UK

£9.99 prime

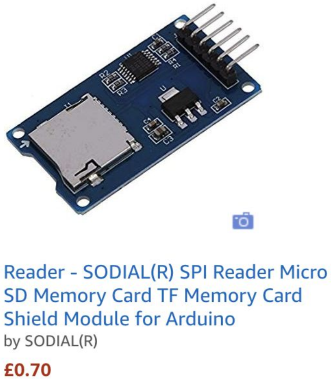
| | |
|---|---|
| 2.99 £ + | Sensor |
| 3.66 £ + | Arduino Nano |
| 3.33 £ + | WiFi module |
| 5.99 £ + | micro SD card |
| 0.70 £ + | SPI card reader |


More options available

Transcend 4GB MicroSDHC Class 4 Memory Card with SD Adaptor

by Transcend

£5.99 prime


Reader - SODIAL(R) SPI Reader Micro SD Memory Card TF Memory Card Shield Module for Arduino

by SODIAL(R)

£0.70

# VIDEO TIME?

Video time!

# Black Hat Sound Bytes

- A covert channel on Android devices that use energy consumption to exfiltrate data
- Low cost attack can be easily deployed on charging stations and power banks
- Turn your device off while recharging

# Acknowledgment

- Laila Abudahi, University of Washington (US)
- Prof. Radha Poovendran, University of Washington (US)
- Prof. Ivan Martinovic, University of Oxford (UK)
- Elia Dal Santo, University of Padua (IT)

UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

Utrecht University

UNIVERSITY OF OXFORD

UNIVERSITY of WASHINGTON

# Questions?

Thank you for your attention!

A covert channel by:

**Riccardo Spolaor** (riccardo.spolaor@cs.ox.ac.uk)
Riccardo Bonafede
Veelasha Moonsamy (Twitter: @veelasha_m)
Mauro Conti (conti@math.unipd.it)