

BO - AUGUST 4, 2016 / MANDALAY BAY / LAS VEGAS



Hacking challenge: steal a car!





Your "local partner in crime"

Sławomir Jasek

- IT security expert securing
- since 2005, and still loves this job



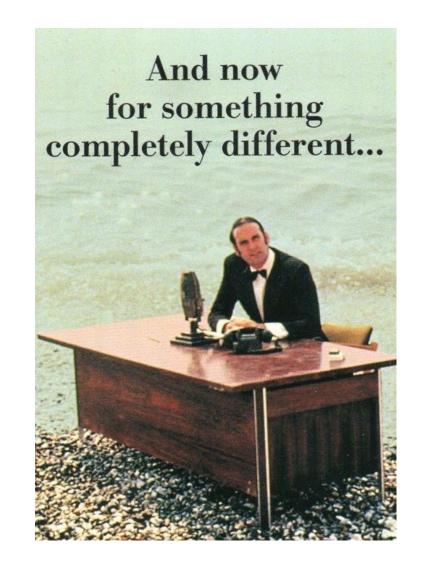
Agenda

- BLE vs security
- How to hack the car
- New tool
- Vulnerabilities examples
 - Smart lock
 - Anti-theft device
 - Mobile PoS
 - Other gadgets
- What can we do better



Bluetooth Smart? (aka Low Energy, 4.0...)

- Probably most thriving IoT technology
 - Wearables, sensors, home automation, household goods, medical devices, door locks, alarms, banking tokens, smart every-things...
- Completely different than previous Bluetooth



BLE (v4.0) security: encryption

- 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
- 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/



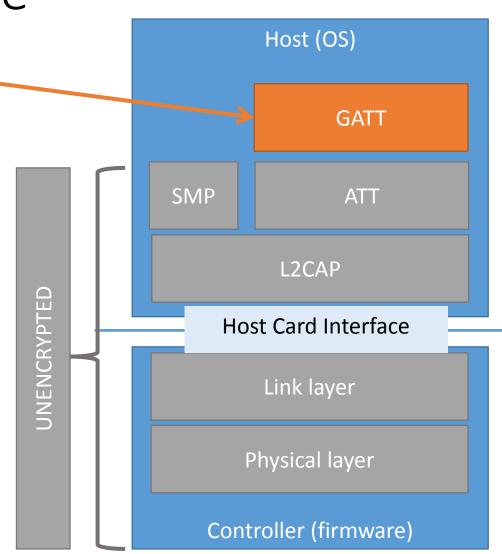
BLE (v4.0) security in practice

- 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 (v4.0) security in 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

?

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

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

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

To protect your transactions from unauthorised access by third parties, operates in accordance with the highest card payment industry security sta

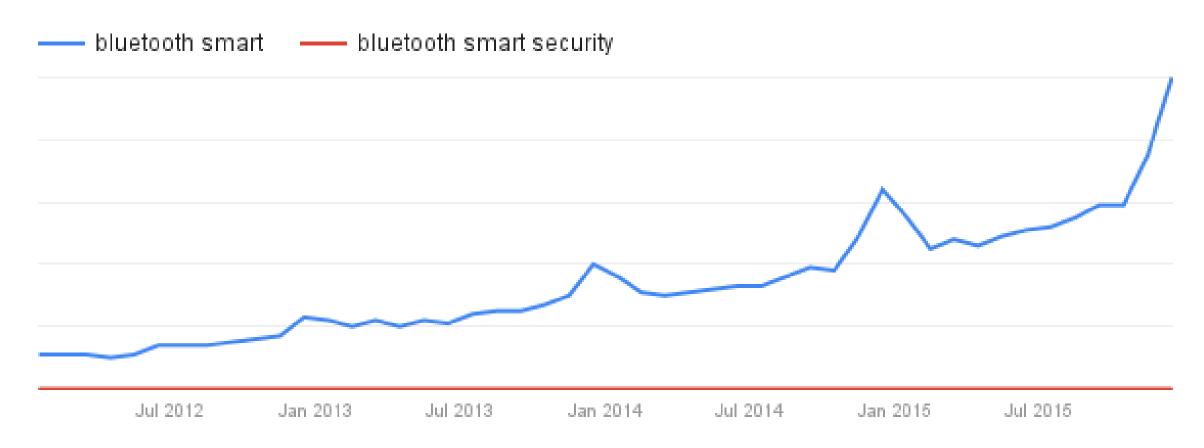
- PCI-DSS (Payment Card Industry Data Security Standard) is the highest of security standard used in the credit card industry concerning data transfer data storage.
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are 'encry protocols' that protect data that is transmitted over the internet.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

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

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



Satisfies regular users, but how about you?







So, how to hack the BLE car lock?

Remote relay?

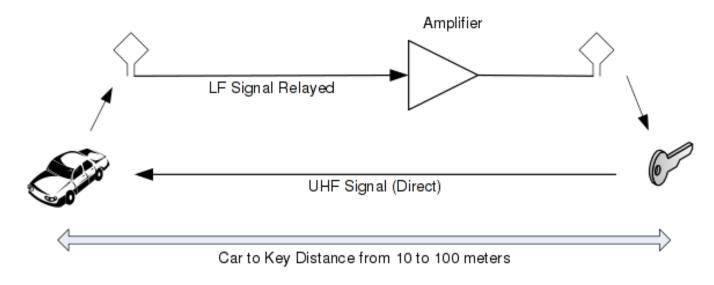


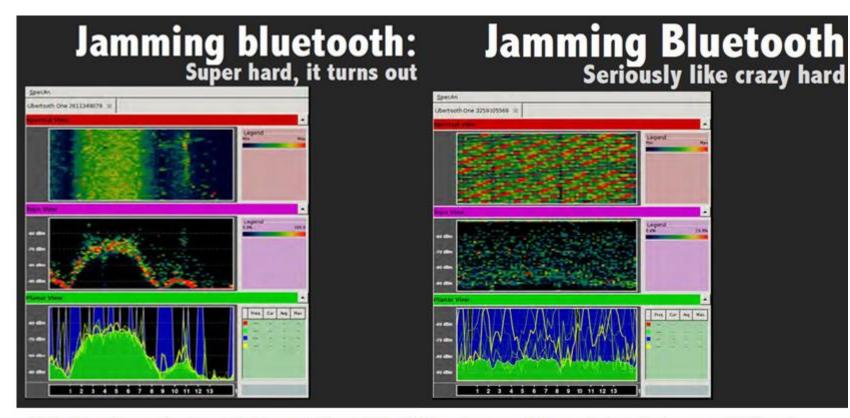
Figure 3. The relay with antennas, cables and an (optional) amplifier.

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



So, how to hack the BLE car lock?

- Remote relay?
- Jamming?
- Brute force?



"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



So, how to hack the BLE car lock?

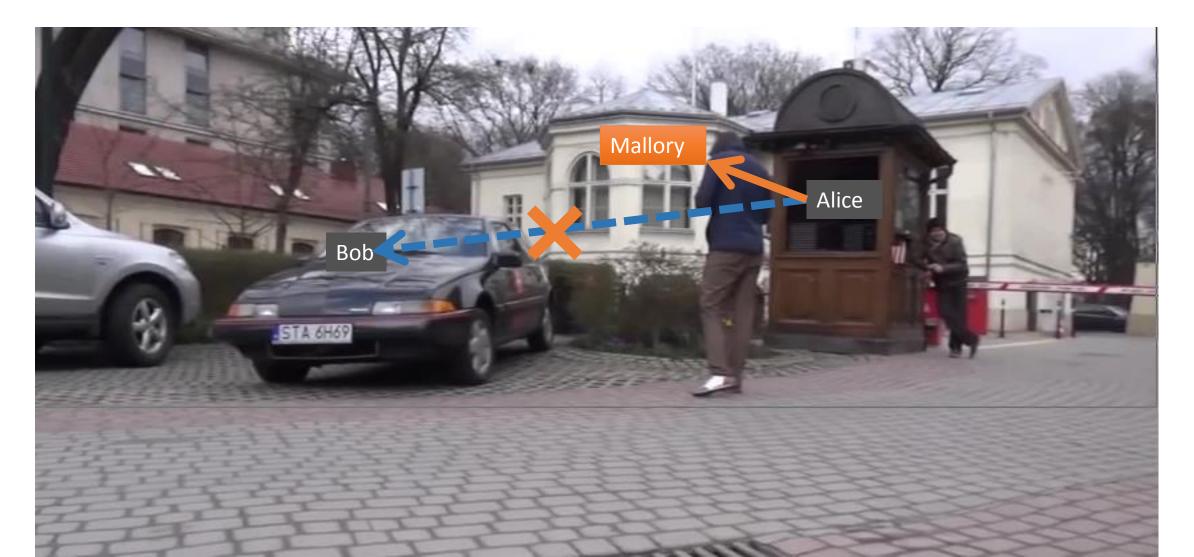
- Remote relay?
- Jamming?
- Brute force?
- BLE sniffing?
- Mobile app analysis?
- ...
- MITM?



http://greatscottgadgets.com/ubertoothone/



Man in the Middle?





How to MITM: isolate the signal?





How to MITM?

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

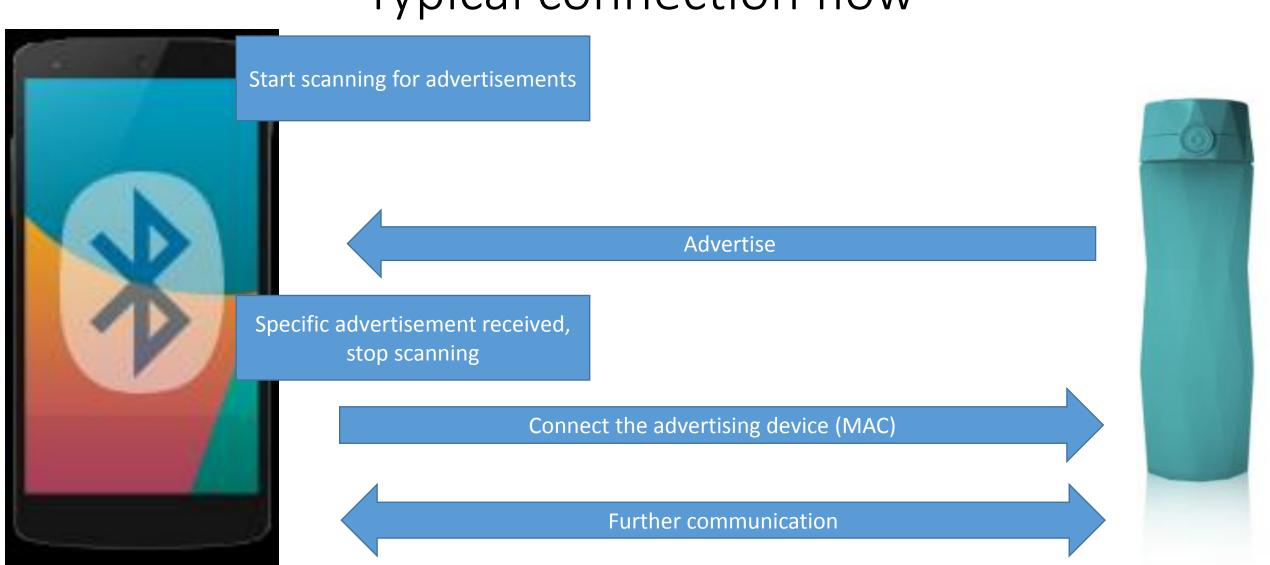
More signals?



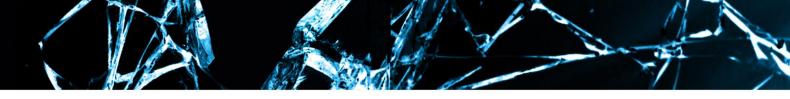
And how to handle them in a single system?



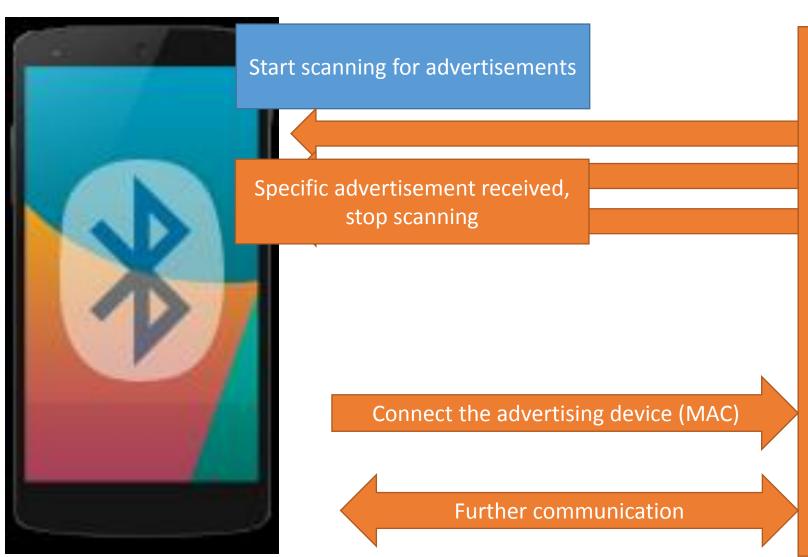
Typical connection flow







MITM



Advertise more frequently

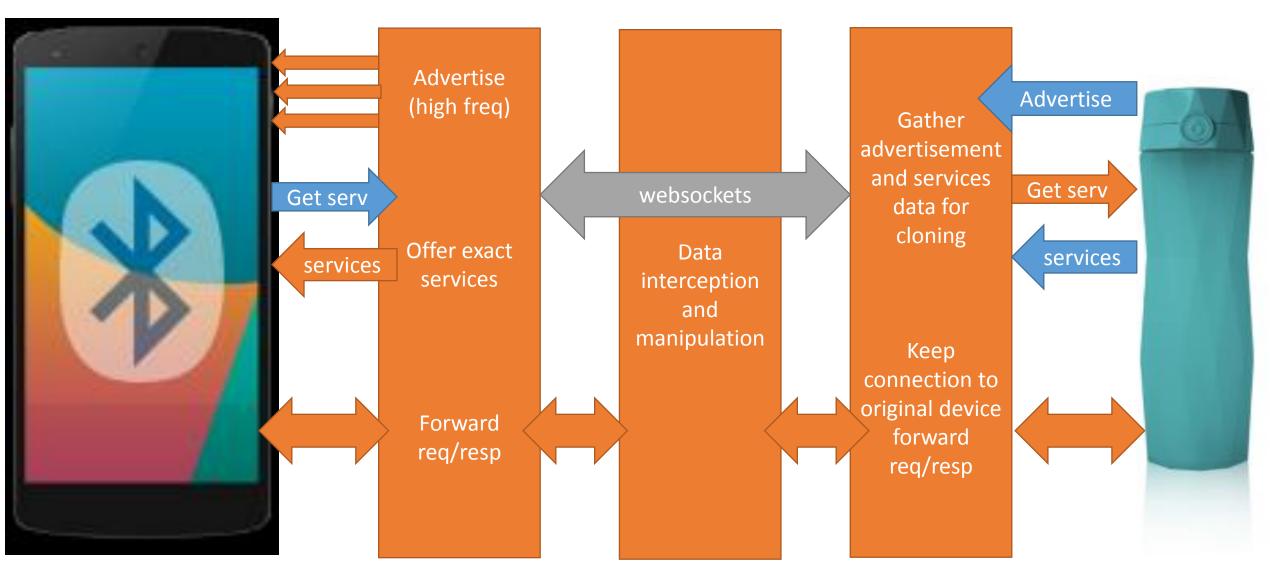
MITM?

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





New tool - architecture





New BLE MITM Tool – a must have for IoT tester!

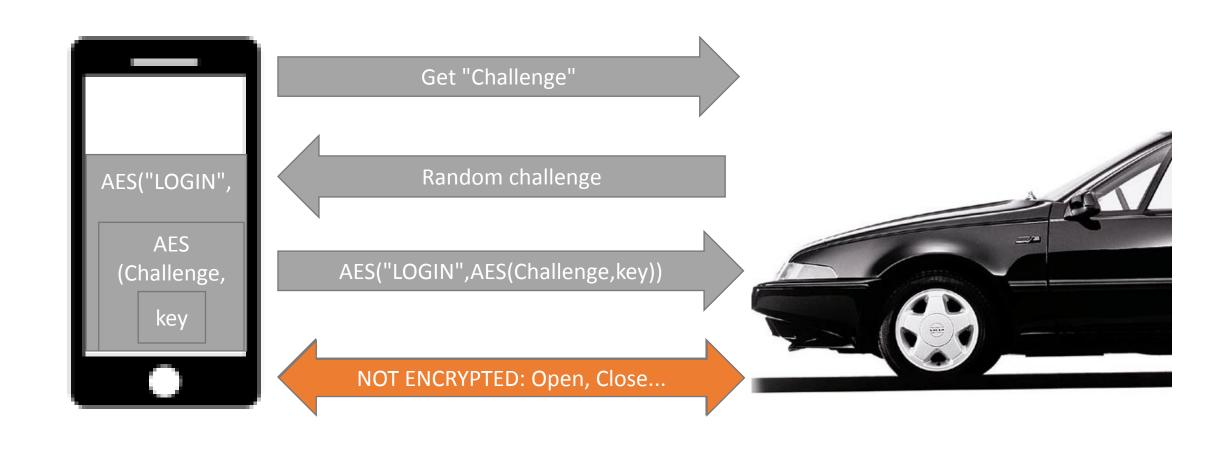
- Open source
- Node.js
- Websockets
- Modular design
- Json
- .io website



And a cool logo!

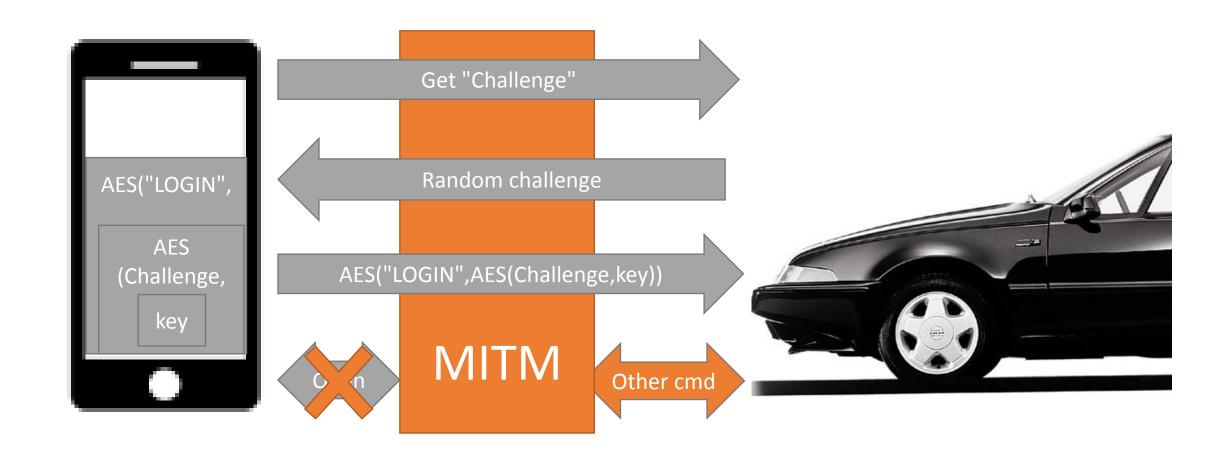


Car hacking challenge: authentication





Authentication: attack?





Other commands (based on mobile app):

- setEngineBlockadeSetting turn on/off
- **setBlinker** blinker sequence unlocking engine
- initConfigMode initiate the configuration overwrite the passwords
- initiateDataTransfer dump the whole configuration (including all passwords)



PRNG?

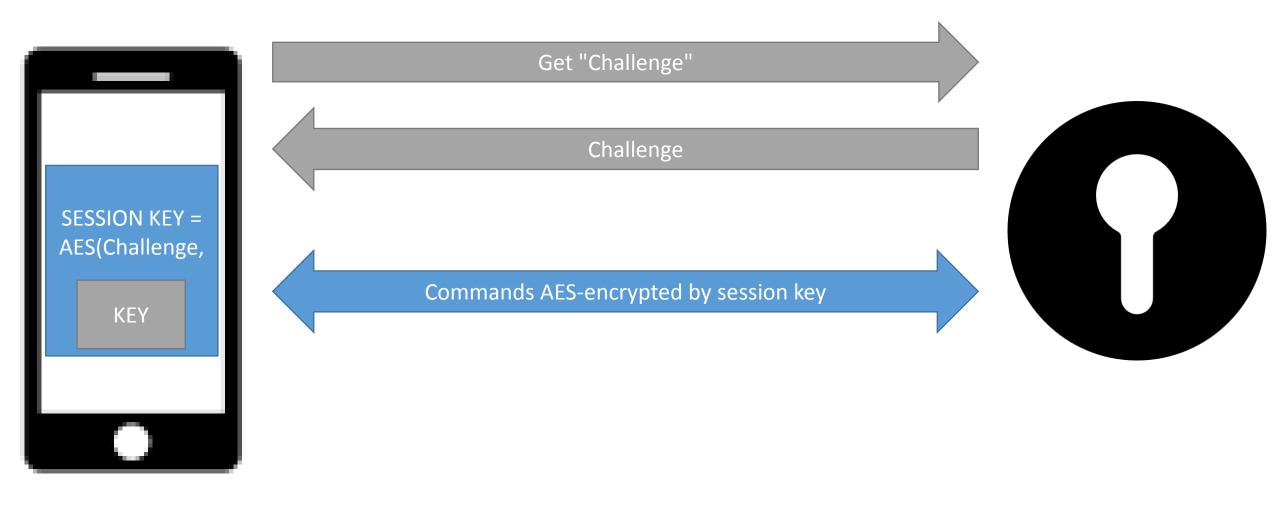
- Is there any function which allows to generate a random number?
- There is no function to do this. However, there is a reasonably good alternative (...), which reads the module's **serial number** and uses the **two** least significant **bytes**, then triggers a channel 14 (**temperature**) ADC read 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)

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?
- Let's take a look at the details...

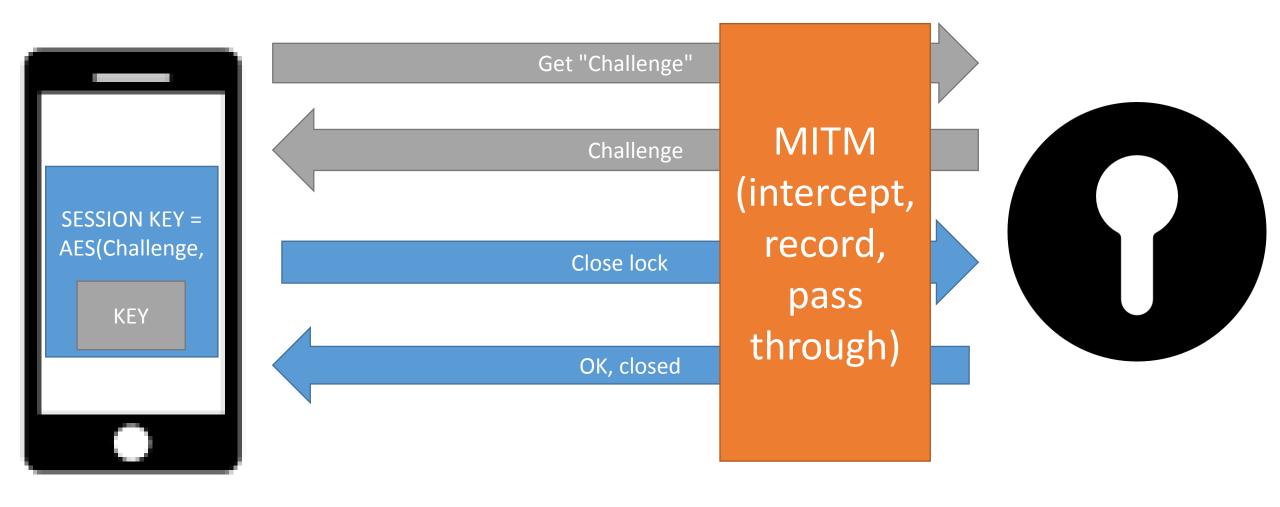


Smart lock - protocol





Smart lock - protocol



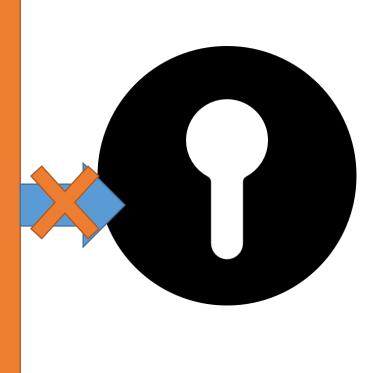


Smart lock – attack

The same as recorded session

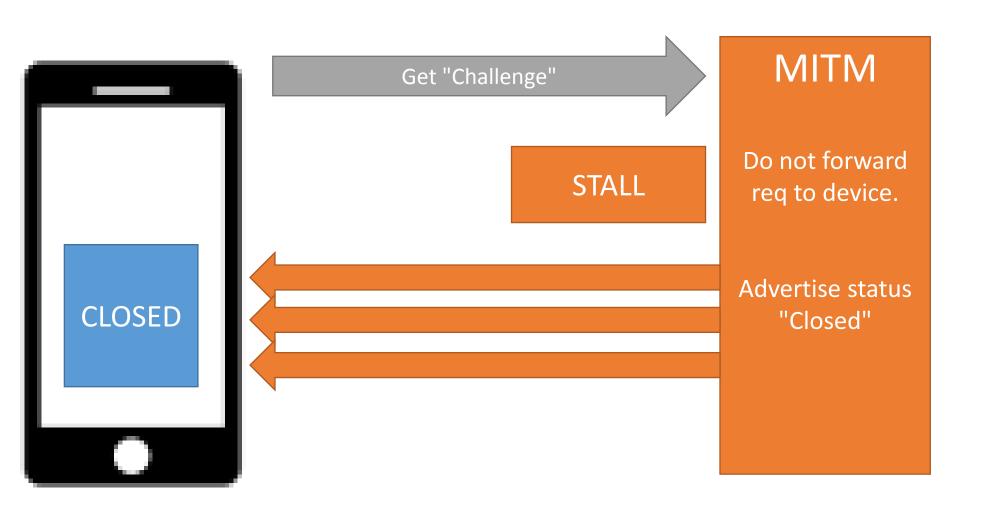


MITM (replay)





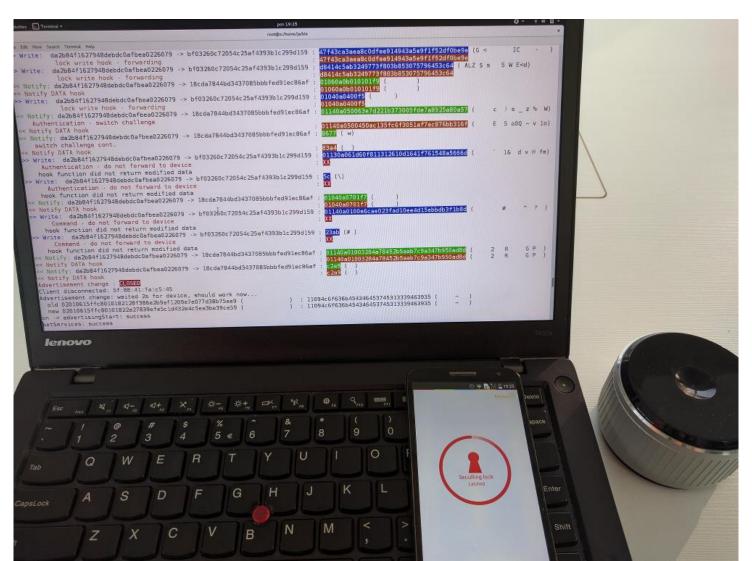
Smart lock – attack v2







Smart lock – DEMO





Smart lock: AT commands

BLE module AT interface exposed

7.2 Reset Commands

7.2.1 Reset (ATRST)

SD RESET

Function: Resets the module.

Command Format: ATRST

Example(s):

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>
```



AT commands

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>
```



AT commands

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



AT commands

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):

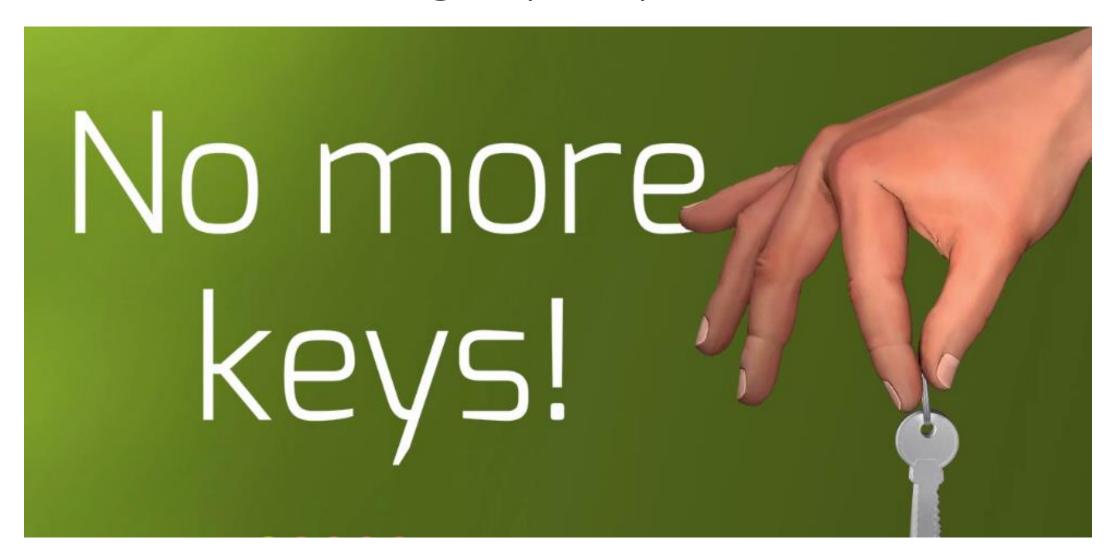
PIO_Num:

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



Fallback to analog key may be unavailable...



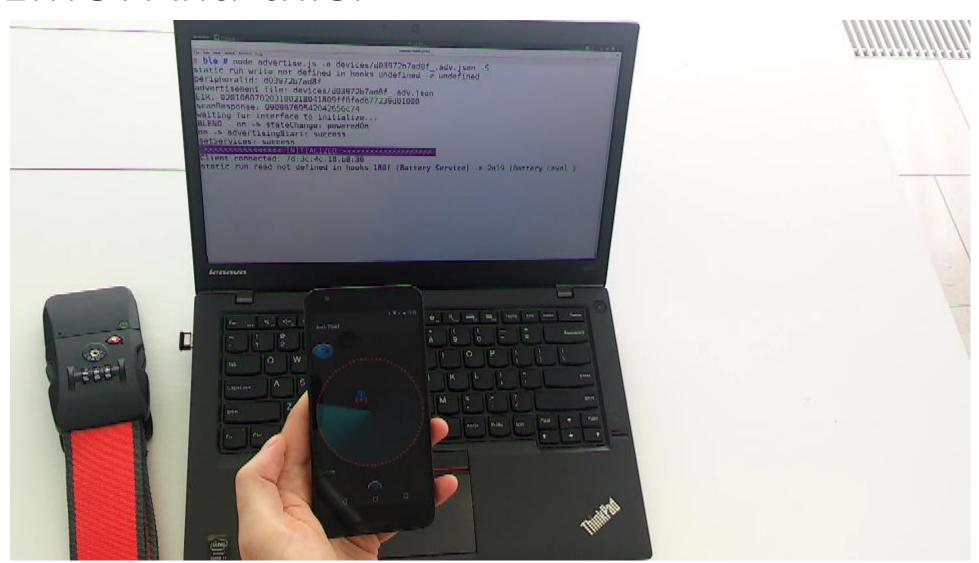


DEMO: AT commands

```
sent CMD: ATSCL?
0K
ATSUART?
Switch to CMD mode
sent CMD: ATSUART?
0K
3,0,0,0
ATT?
Switch to CMD mode
sent CMD: ATT?
0K
027,081
ATSN?
Switch to CMD mode
sent CMD: ATSN?
0K
LockECFE7E139F95
```



DEMO: Anti-thief



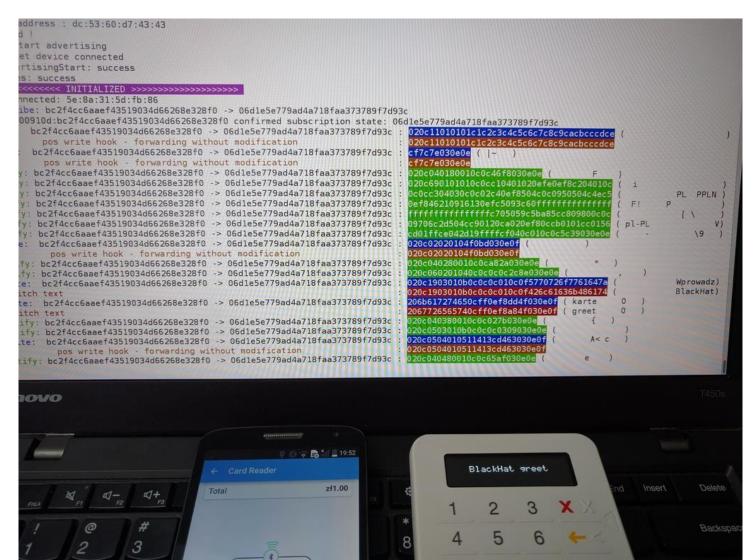




```
Static - start advertising
     target device connected
on -> advertisingStart: success
setServices: success
Client connected: 4f:66:59:38:16:eb
Read: 180f (Battery Service) -> 2a19 (Battery Level ) : 45 (B)
>> Subscribe: 0d583600447b98d61f6ec3340bdfbab8 -> 0d583601447b98d61f6ec3340bdfbab8
  da8c352442be:0d583600447b98d61f6ec3340bdfbab8 confirmed subscription state: 0d583601447b98d6
>> Write: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583701447b98d61f6ec3340bdfbab8 : 123456 ( 4V)
Read: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583711447b98d61f6ec3340bdfbab8 : 01 ( )
Read: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583708447b98d61f6ec3340bdfbab8 : 06
<< Read: 1803 (Link Loss) -> 2a06 (Alert Level ) : 00 ( )
>> Write: 1802 (Immediate Alert) -> 2a06 (Alert Level ) : 01 ( )
>> Write: 1802 (Immediate Alert) -> 2a06 (Alert Level ) : 01 (
>> Write: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583707447b98d61f6ec3340bdfbab8 : 536d6172744669
000000 (SmartFinde
>> Write: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583701447b98d61f6ec3340bdfbab8 : 666666 (fff)
Read: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583711447b98d61f6ec3340bdfbab8 : 01 ( )
>> Write: 1802 (Immediate Alert) -> 2a06 (Alert Level ) : 01 ( )
Read: 0d583700447b98d61f6ec3340bdfbab8 -> 0d583708447b98d61f6ec3340bdfbab8 : 06 ( )
<< Read: 1803 (Link Loss) -> 2a06 (Alert Level ) : 00 ( )
Client disconnected: 4f:66:59:38:16:eb
lenovo
```

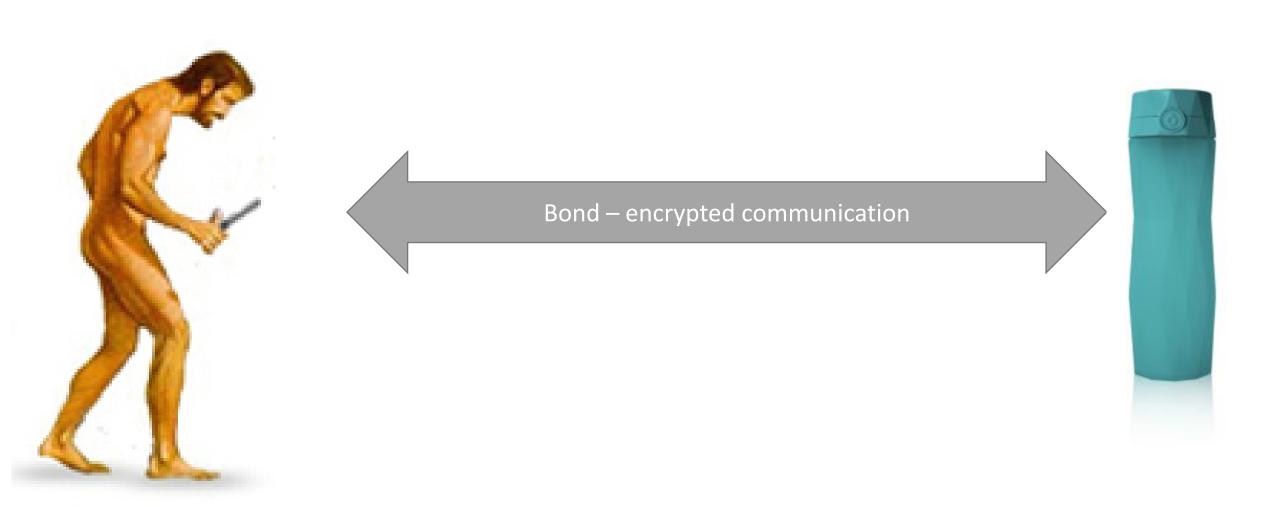


DEMO: Mobile PoS



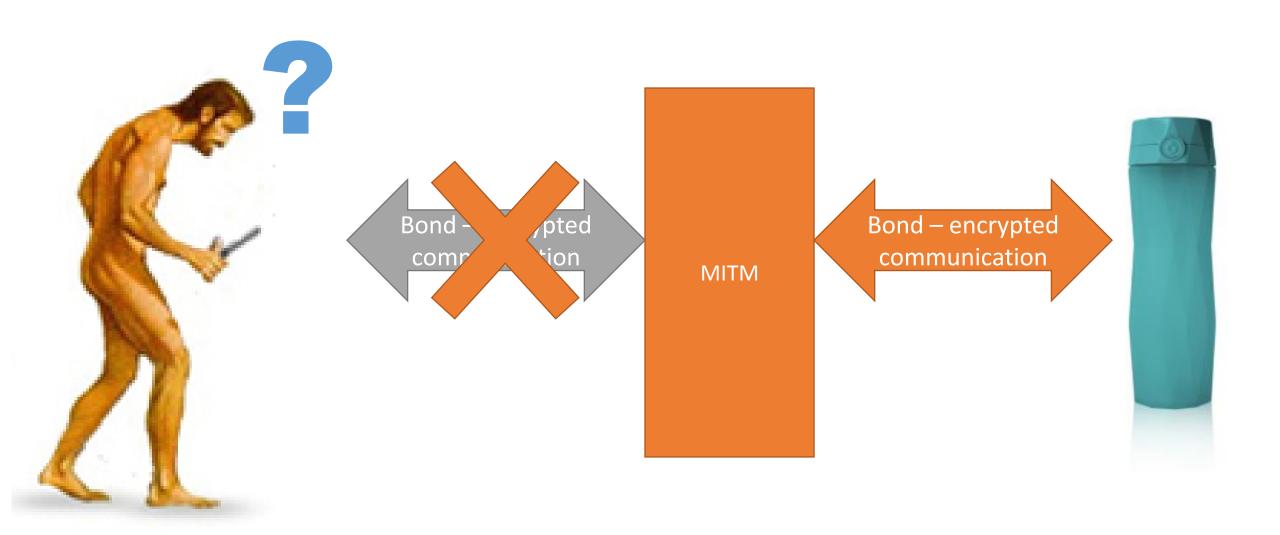


But what about BLE encryption?





"Just Works"

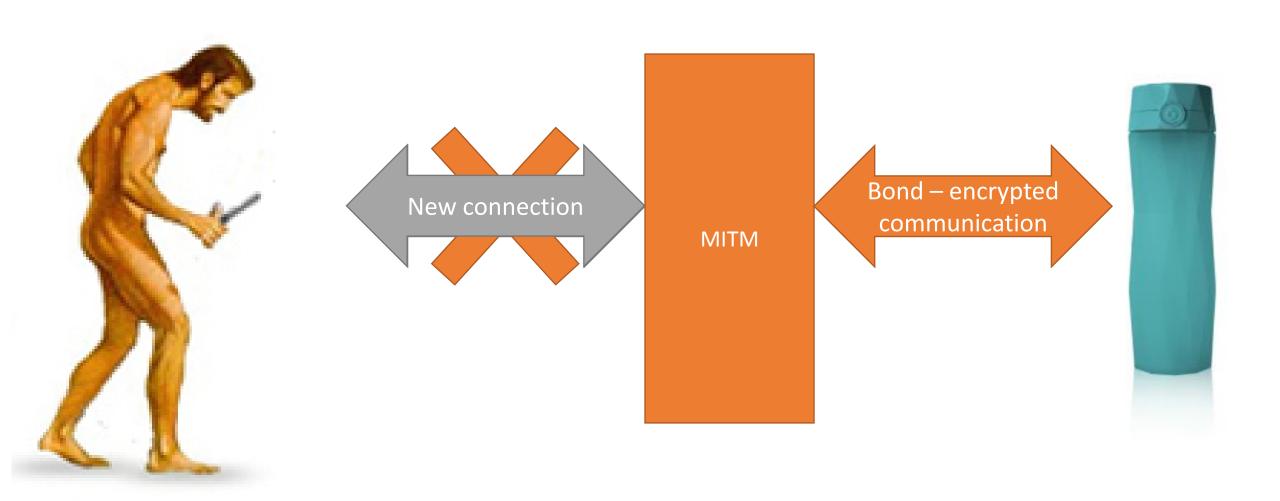




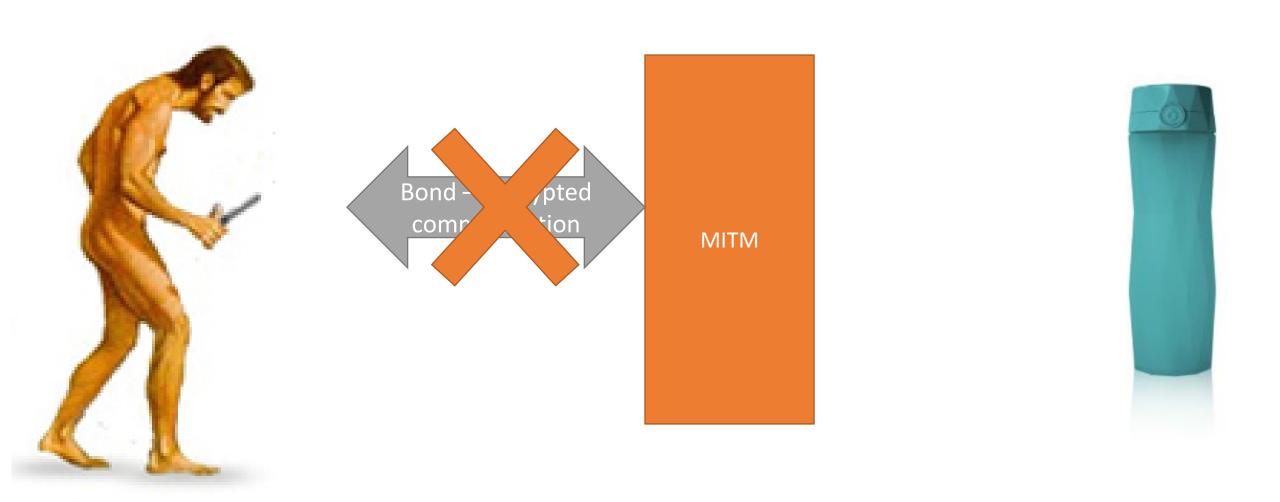




Remove pairing, new connection with MITM

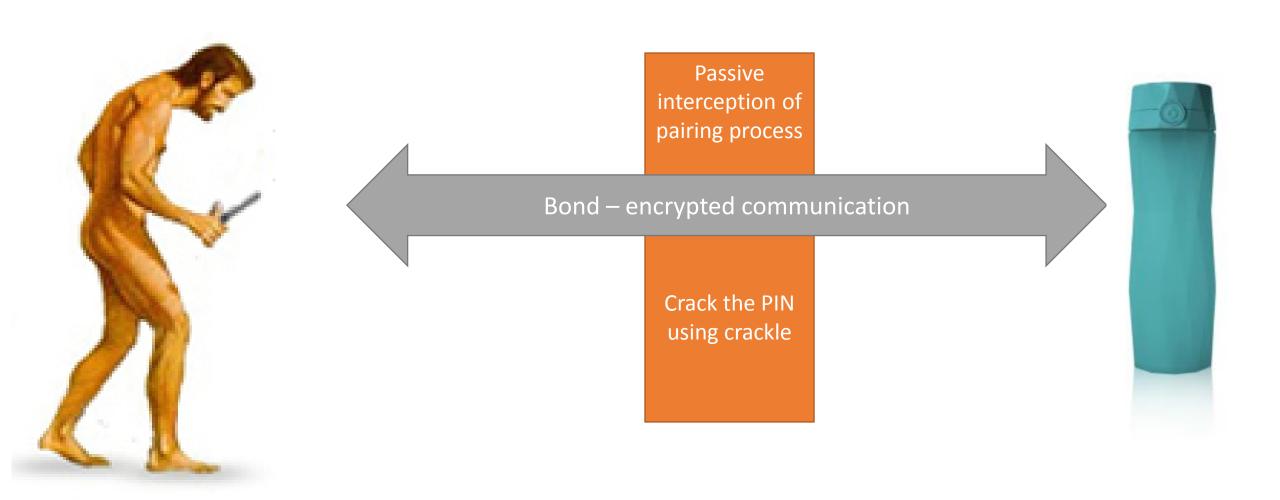


PIN entry – trick into pairing again, sniff, crack





PIN entry – trick into pairing again, sniff, crack





Some attacks

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





Risk? It depends...

- 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



Barack Obama

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











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-fitnesstracker-represent-national-security-risk-1492705



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



Q&A?

More information, these slides, whitepaper, videos, tool source code:

