KU LEUVEN

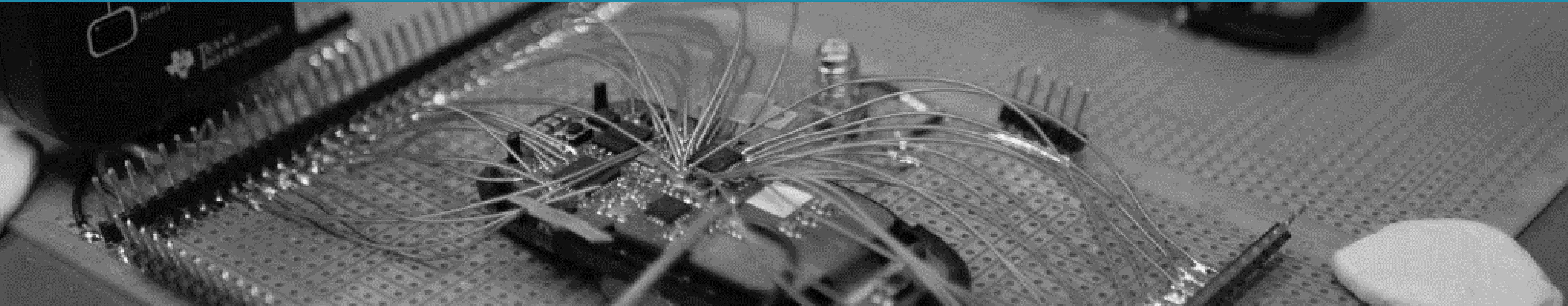
My other car is your car:

Compromising the Tesla Model X keyless entry system

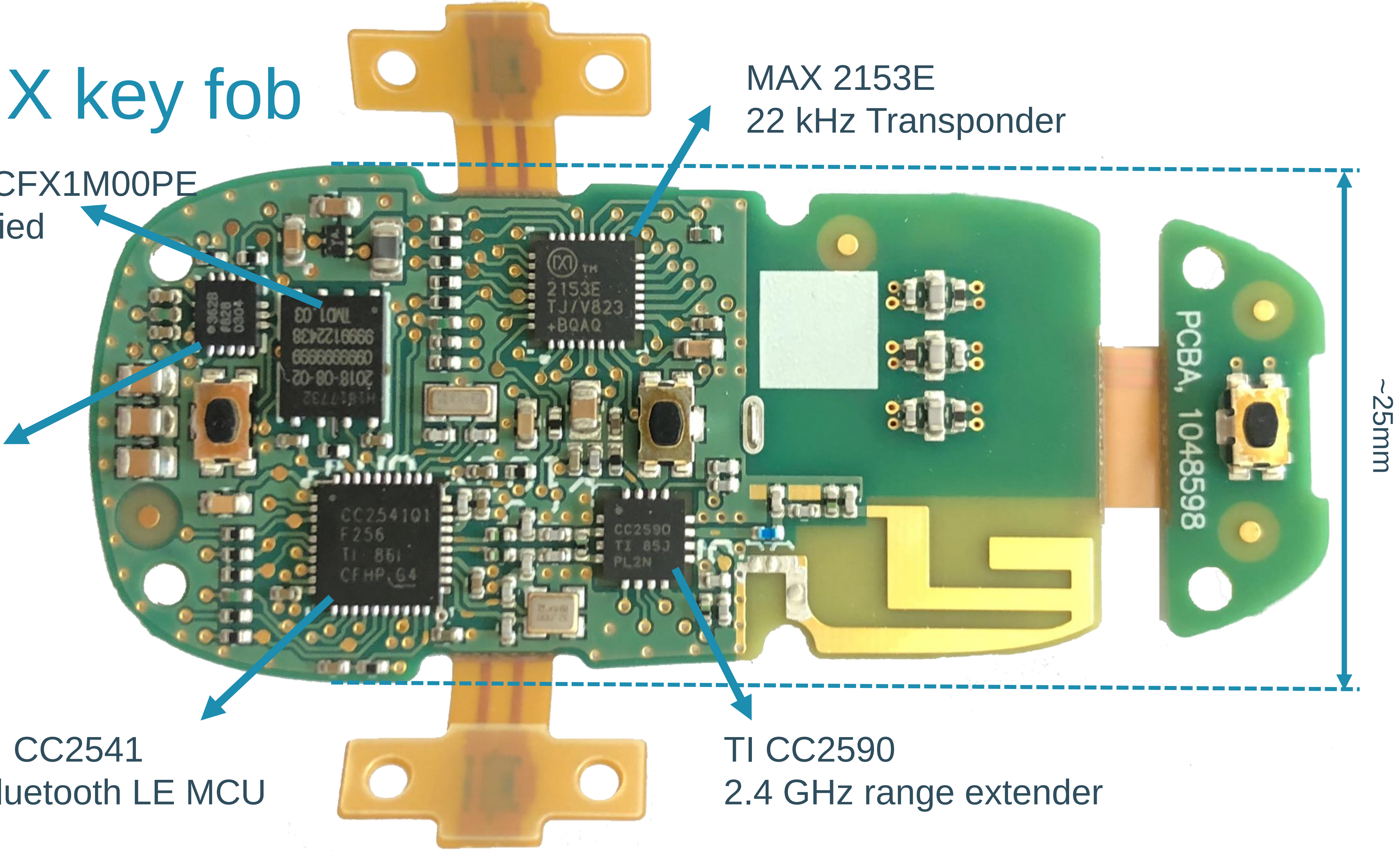
Lennert Wouters, Benedikt Gierlichs and Bart Preneel

Real World Crypto 2021

COSIC



Model X key fob



Infineon SLM97CFX1M00PE
CC EAL5+ certified

MAX 2153E
22 kHz Transponder

ADXL362B
Accelerometer

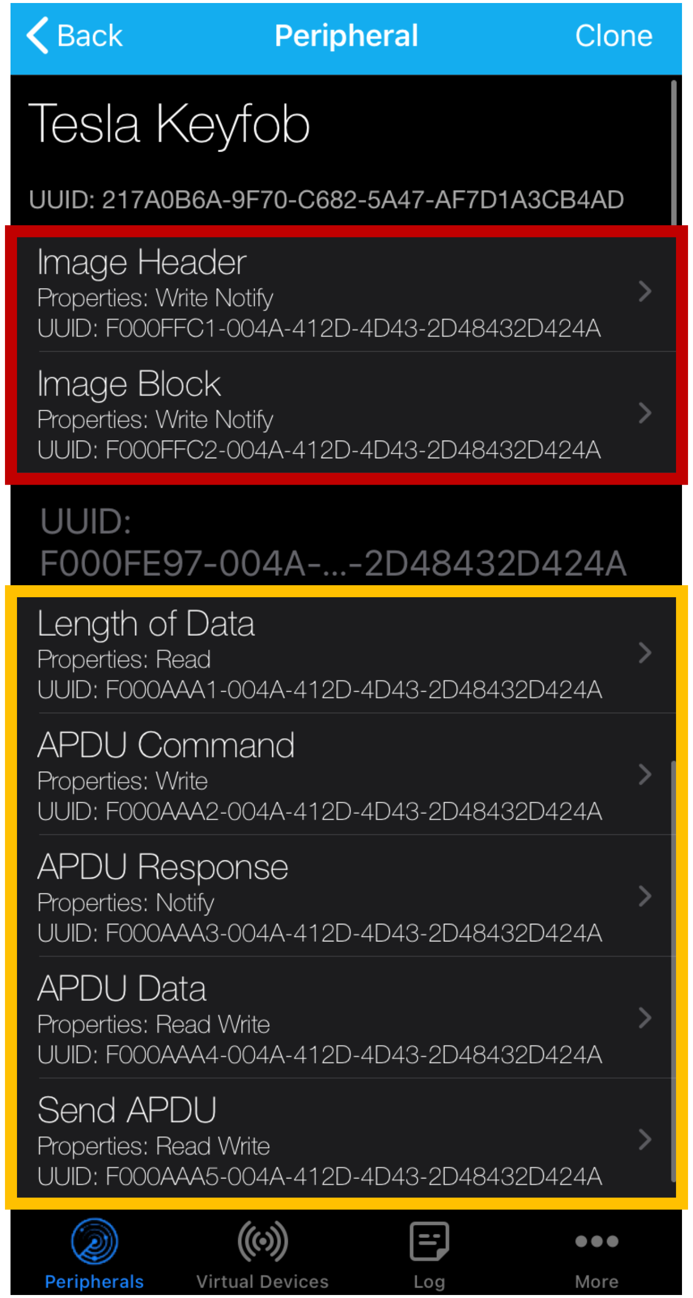
~25mm

TI CC2541
Bluetooth LE MCU

TI CC2590
2.4 GHz range extender

BLE Interface

- Key fob is a BLE peripheral
- Reseat the battery (power cycle)
  - Key fob advertises as connectable
- Over-Air-Download
  - Slightly modified compared to the example implementation
  - **Improper signature validation**
- Application Protocol Data Unit Interface
  - Allows to send APDU commands to the SE over BLE
  - **Some APDUs blocked**



Tesla Keyfob

UUID: 217A0B6A-9F70-C682-5A47-AF7D1A3CB4AD

Image Header
Properties: Write Notify
UUID: F000FFC1-004A-412D-4D43-2D48432D424A

Image Block
Properties: Write Notify
UUID: F000FFC2-004A-412D-4D43-2D48432D424A

UUID:
F000FE97-004A-...-2D48432D424A

Length of Data
Properties: Read
UUID: F000AAA1-004A-412D-4D43-2D48432D424A

APDU Command
Properties: Write
UUID: F000AAA2-004A-412D-4D43-2D48432D424A

APDU Response
Properties: Notify
UUID: F000AAA3-004A-412D-4D43-2D48432D424A

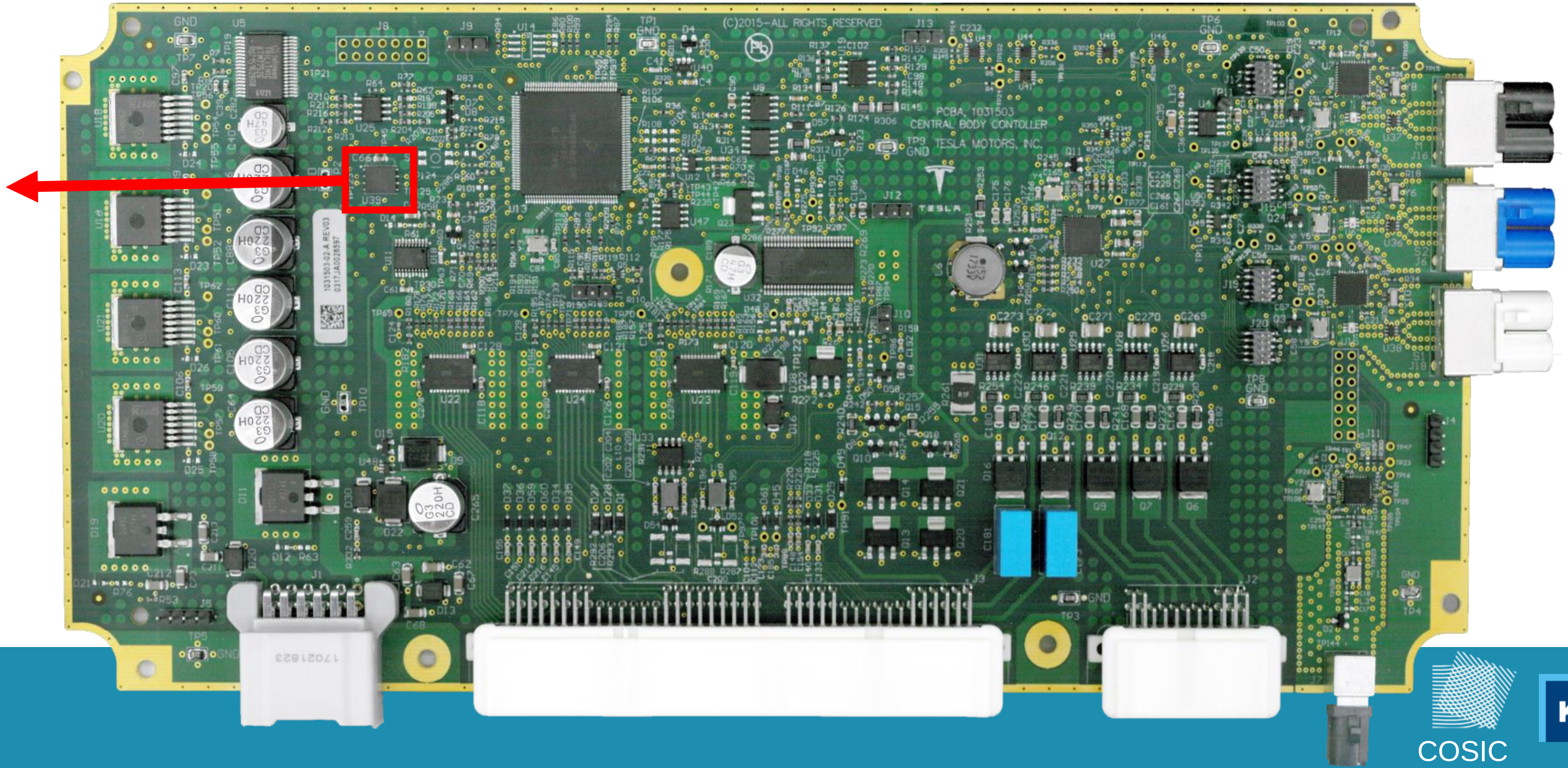
APDU Data
Properties: Read Write
UUID: F000AAA4-004A-412D-4D43-2D48432D424A

Send APDU
Properties: Read Write
UUID: F000AAA5-004A-412D-4D43-2D48432D424A

Force key fob wake-up

- Body Control Module can send a wake-up command over LF
- Allows a car to wake-up key fobs that have been paired to it
  - Based on an identifier derived from the VIN

Model X BCM PCB



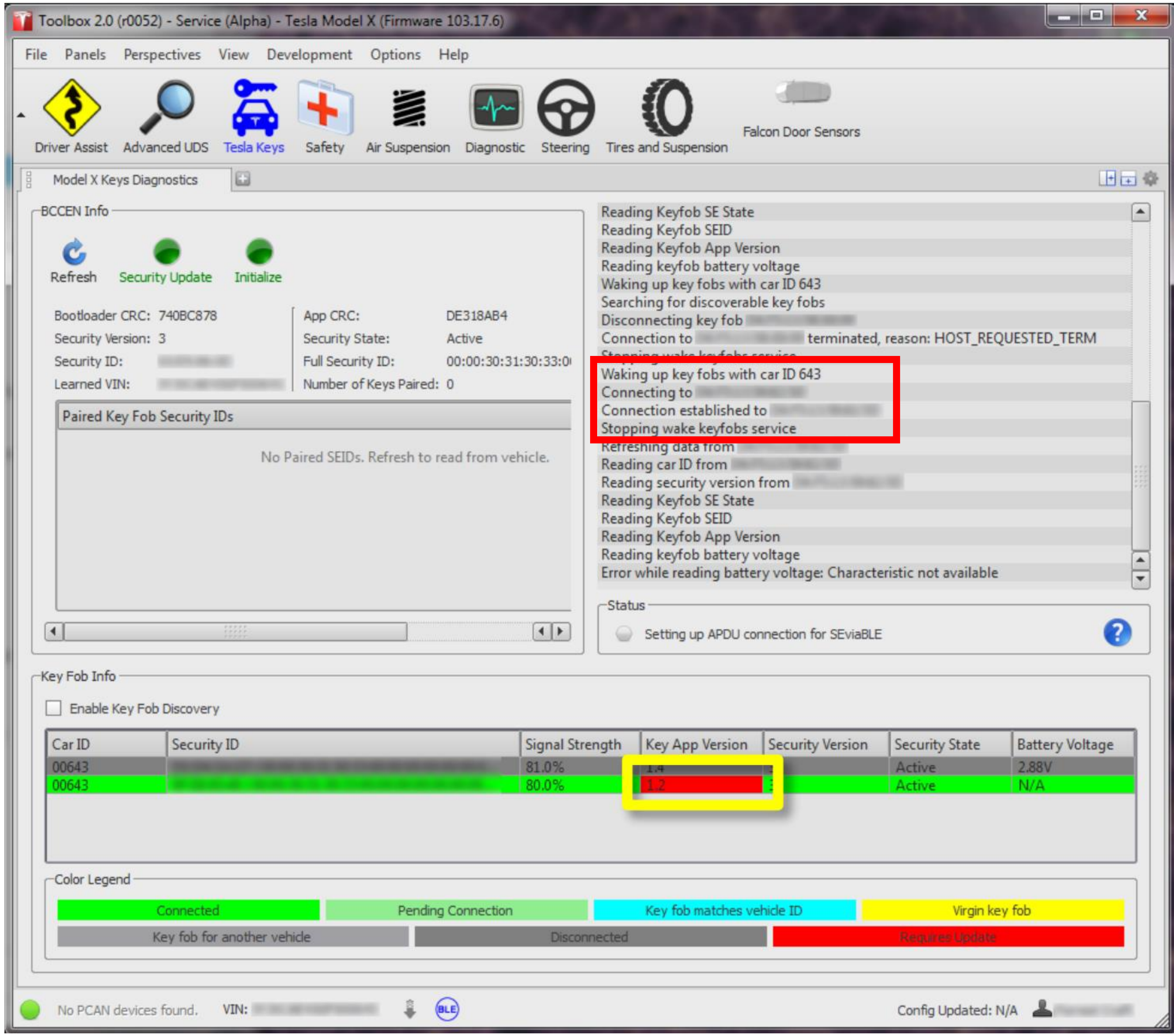
Infineon SLM97CFX1M00PE
Stores VIN

Plan of attack

1. Request target key fob to advertise as connectable
   - Can be achieved using a modified BCM
2. Connect to the key fob and push malicious firmware
   - Firmware is modified to allow all APDUs
3. Request a valid rolling code through the BLE APDU interface
4. Use the acquired rolling code to unlock the car
   - This code can only be used to unlock the car

Toolbox

- Used for servicing Model S and X
- Not publicly available
  - Available 'on the internet'
  - Briefly (unintentionally?) released
- Interesting parts are stored encrypted
  - must be decrypted before use ;)



Bootloader CRC: 740BC878
Security Version: 3
Security ID: [redacted]
Learned VIN: [redacted]

App CRC: DE318AB4
Security State: Active
Full Security ID: 00:00:30:31:30:33:0
Number of Keys Paired: 0

No Paired SEIDs. Refresh to read from vehicle.

```
Reading Keyfob SE State
Reading Keyfob SEID
Reading Keyfob App Version
Reading keyfob battery voltage
Waking up key fobs with car ID 643
Searching for discoverable key fobs
Disconnecting key fob [redacted]
Connection to [redacted] terminated, reason: HOST_REQUESTED_TERM
Stopping wake keyfobs service
Waking up key fobs with car ID 643
Connecting to [redacted]
Connection established to [redacted]
Stopping wake keyfobs service
Refreshing data from [redacted]
Reading car ID from [redacted]
Reading security version from [redacted]
Reading Keyfob SE State
Reading Keyfob SEID
Reading Keyfob App Version
Reading keyfob battery voltage
Error while reading battery voltage: Characteristic not available
```

Status

Setting up APDU connection for SEviaBLE

☐ Enable Key Fob Discovery

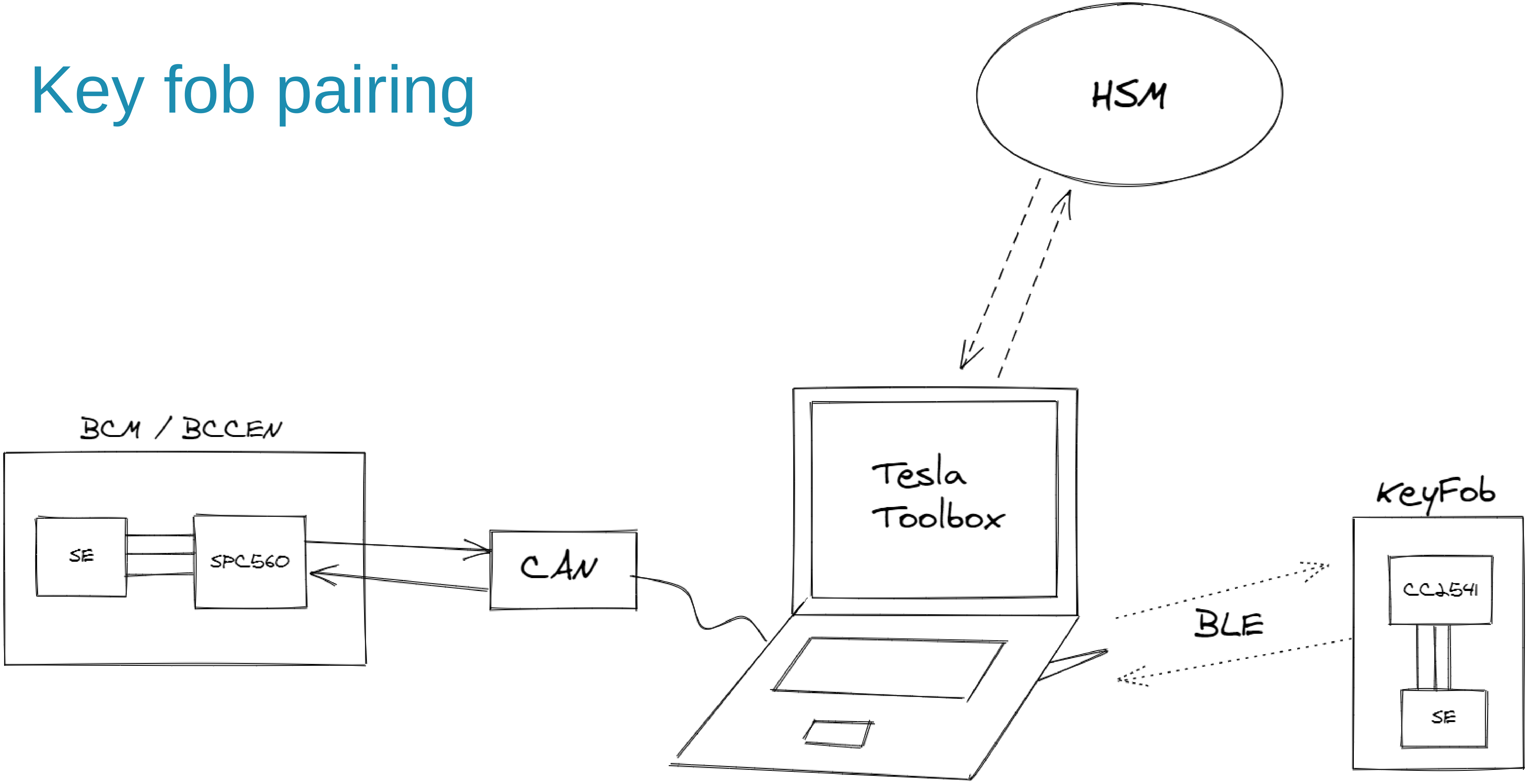
Car ID	Security ID	Signal Strength	Key App Version	Security Version	Security State	Battery Voltage
00643	[redacted]	81.0%	1.4	[illegible]	Active	2.88V
00643	[redacted]	80.0%	1.2	3	Active	N/A

No PCAN devices found. VIN: [redacted]

Config Updated: N/A [redacted]

Picture source: https://static.nhtsa.gov/odi/tsbs/2016/SB-10081823-5448.pdf
Unintentional Toolbox release: https://twitter.com/greentheonly/status/1334564079264993281

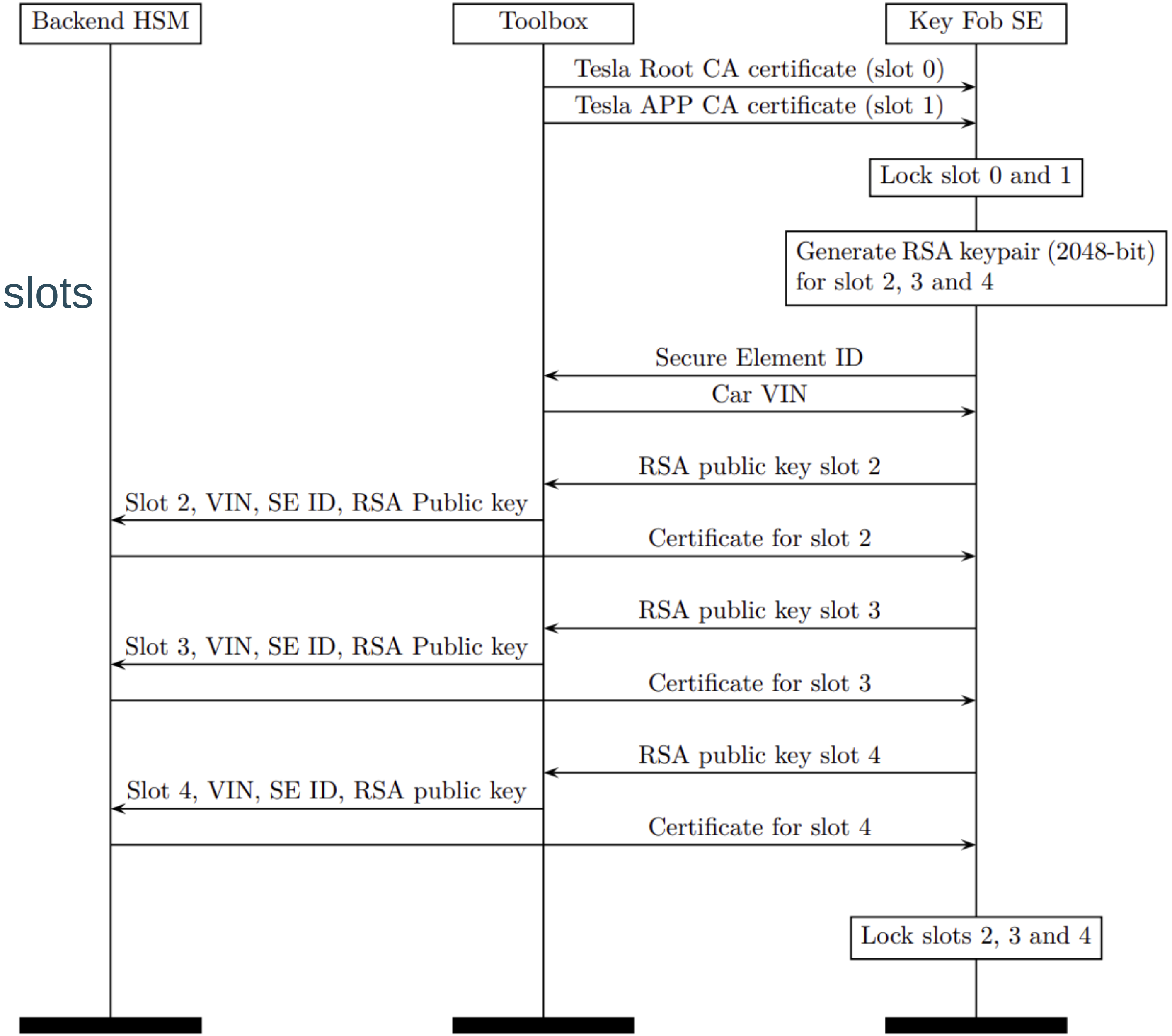
Key fob pairing



Provisioning

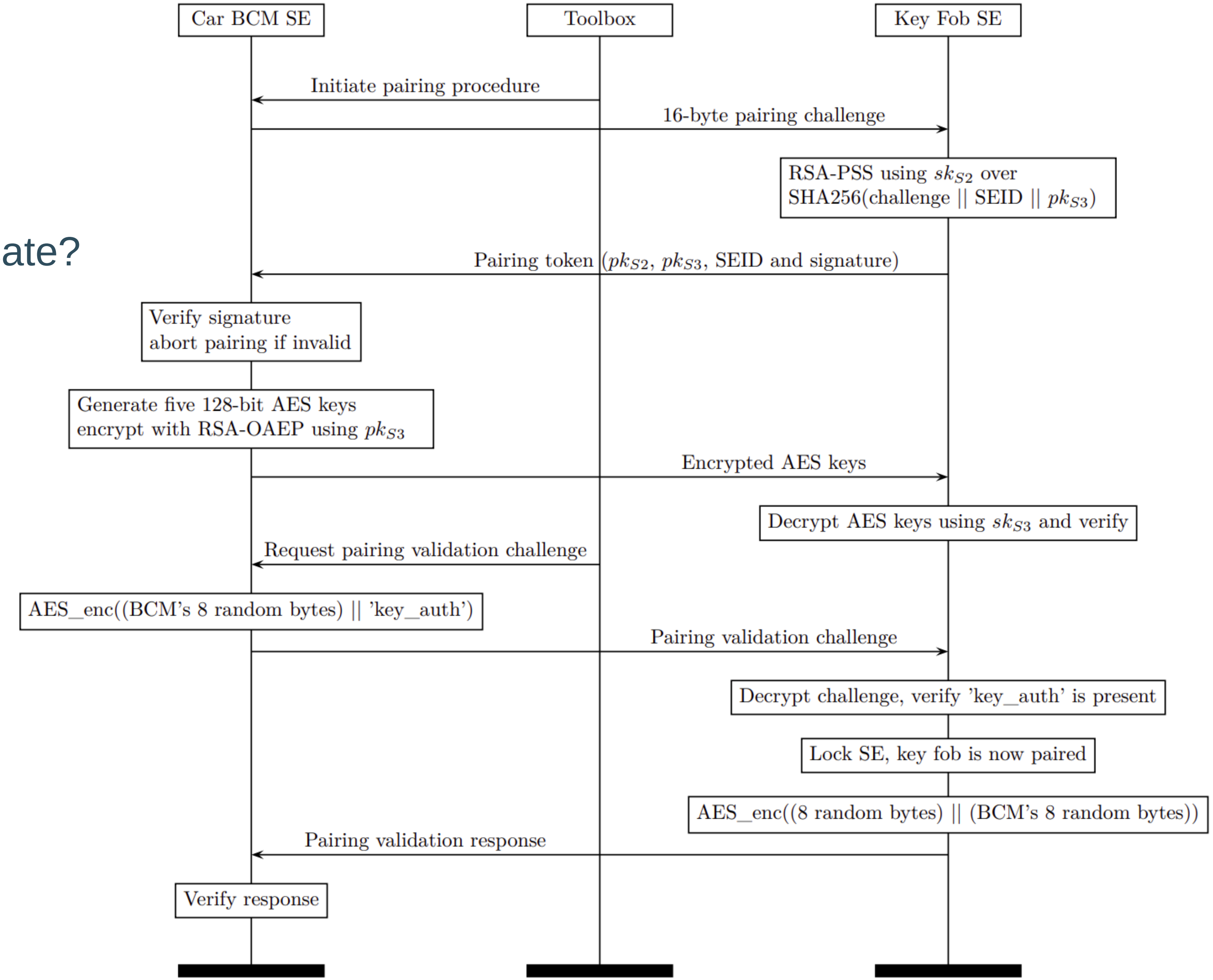
- Key fob Secure Element (SE) has 5 RSA slots
  - Slot 0 and 1: Tesla CA certificates
  - Slot 2, 3 and 4: key fob specific

- HSM signs certificate for slot 2, 3 and 4
  - Presumably so the car can ensure it is pairing to a legitimate key fob
  - Certificates are stored in key fob SE


Backend HSM
Toolbox
Key Fob SE
Tesla Root CA certificate (slot 0)
Tesla APP CA certificate (slot 1)
Lock slot 0 and 1
Generate RSA keypair (2048-bit) for slot 2, 3 and 4
Secure Element ID
Car VIN
RSA public key slot 2
Slot 2, VIN, SE ID, RSA Public key
Certificate for slot 2
RSA public key slot 3
Slot 3, VIN, SE ID, RSA Public key
Certificate for slot 3
RSA public key slot 4
Slot 4, VIN, SE ID, RSA public key
Certificate for slot 4
Lock slots 2, 3 and 4

Pairing

- Where’s ~~Wally/Waldo~~ the certificate?



Car BCM SE

Toolbox

Key Fob SE

Initiate pairing procedure

16-byte pairing challenge

RSA-PSS using sk_{S2} over SHA256(challenge || SEID || pk_{S3})

Pairing token (pk_{S2}, pk_{S3}, SEID and signature)

Verify signature
abort pairing if invalid

Generate five 128-bit AES keys
encrypt with RSA-OAEP using pk_{S3}

Encrypted AES keys

Decrypt AES keys using sk_{S3} and verify

Request pairing validation challenge

AES_enc((BCM’s 8 random bytes) || ’key_auth’)

Pairing validation challenge

Decrypt challenge, verify ’key_auth’ is present

Lock SE, key fob is now paired

AES_enc((8 random bytes) || (BCM’s 8 random bytes))

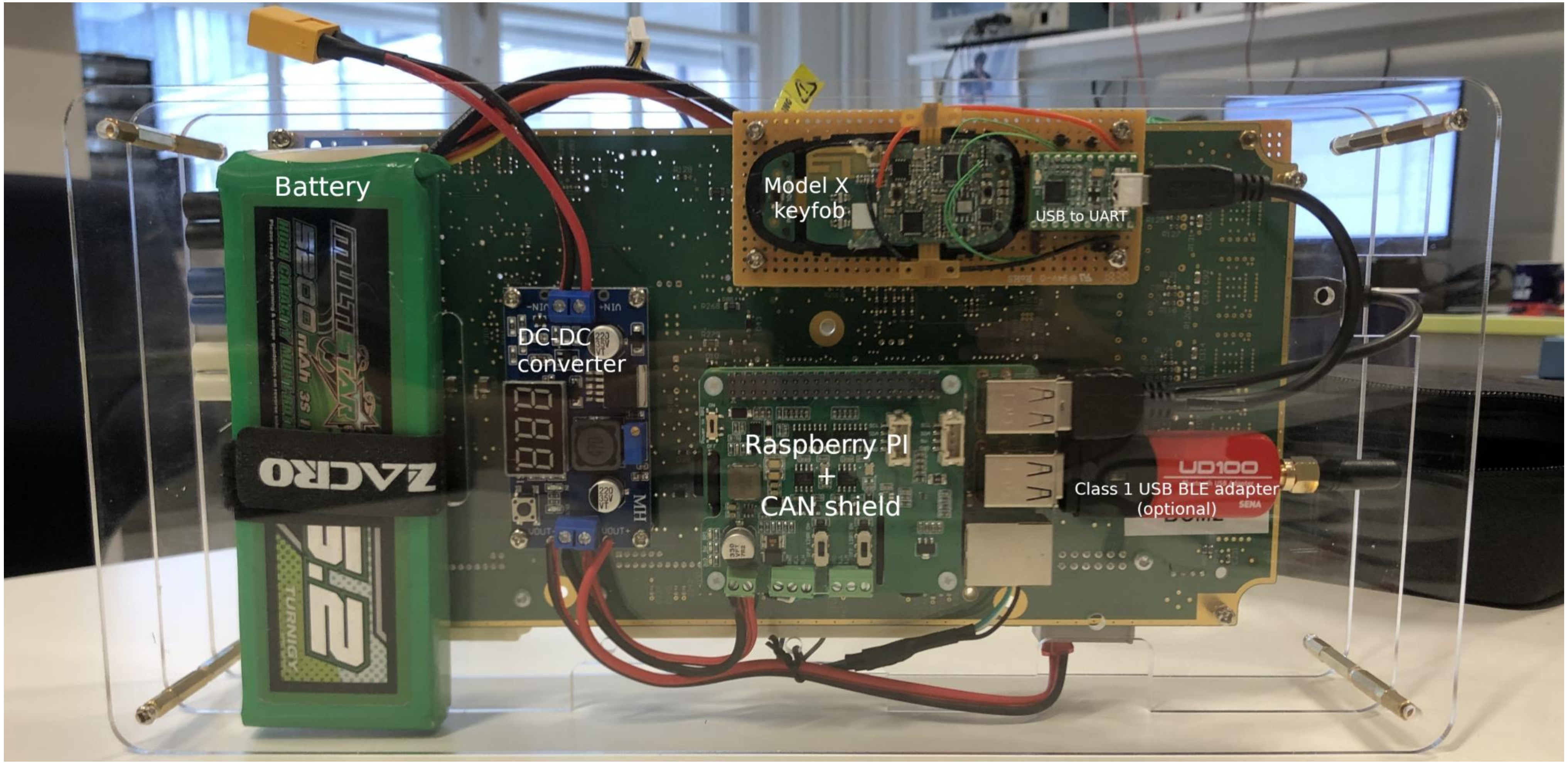
Pairing validation response

Verify response

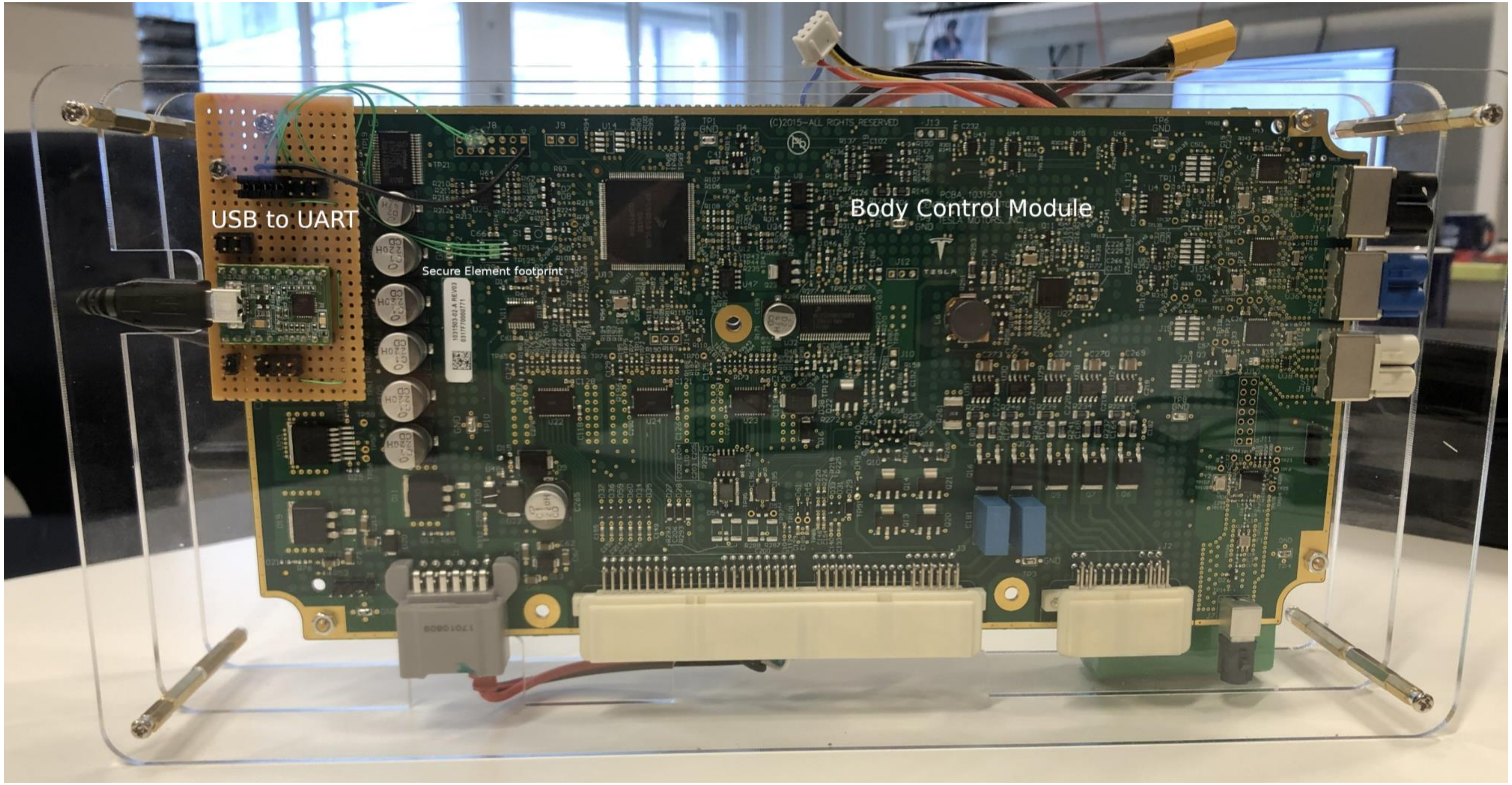
Plan of attack

1. Request target key fob to advertise as connectable
   - Can be achieved using a modified BCM
2. Connect to the key fob and push malicious firmware
   - Firmware is modified to allow all APDUs
3. Request a valid rolling code through the BLE APDU interface
4. Use the acquired rolling code to unlock the car
   - This code can only be used to unlock the car
5. Connect to the diagnostic port and pair a modified key fob to the car
   - Key fob is modified by replacing the secure element

Proof of Concept

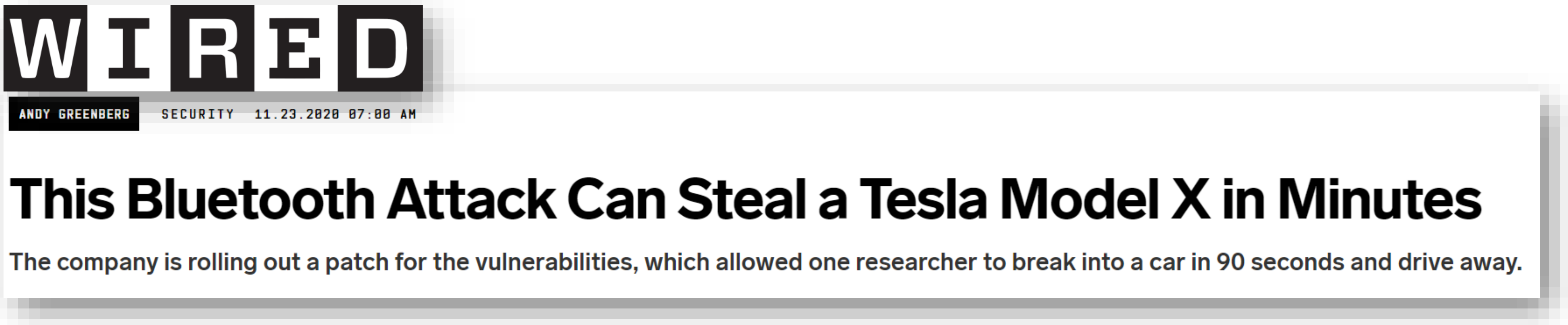


Proof of Concept



Disclosure timeline

- Initial disclosure: August 17 2020
- Patch release: November 2020 (update 2020.48)
- Bounty: $5000



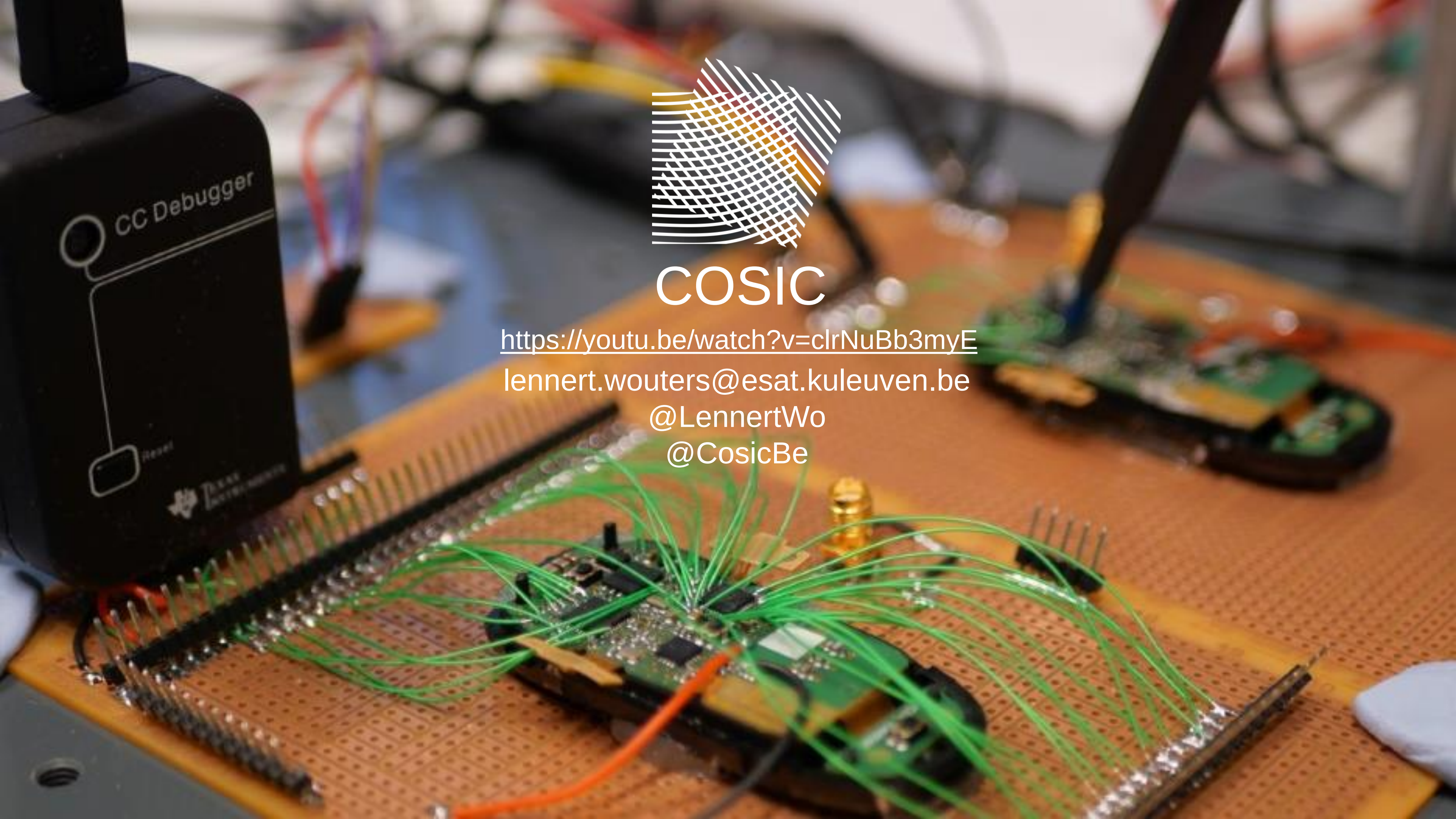
WIRED

ANDY GREENBERG SECURITY 11.23.2020 07:00 AM

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

The company is rolling out a patch for the vulnerabilities, which allowed one researcher to break into a car in 90 seconds and drive away.

https://youtu.be/watch?v=clrNuBb3myE



COSIC

https://youtu.be/watch?v=clrNuBb3myE

lennert.wouters@esat.kuleuven.be

@LennertWo

@CosicBe