

On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats

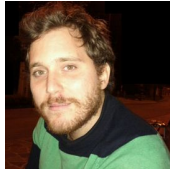


ASRG WORLD Series Webinar, July 2022

Daniele Antonioli (EURECOM)



Daniele Antonioli



- Assistant professor at [EURECOM](#) (France)
- Research on system security
 - **Mobile** (Android, iOS)
 - **Wireless** (Bluetooth, Wi-Fi, proprietary)
 - **Embedded** (trackers, automotive)
 - **Cyber-Physical System** (OT, ICS)
- More info in my [website](#)

Talk Outline

- First study of **protocol-level** Bluetooth threats for vehicles
 - Unexplored but relevant attack surface
- **Methodology** to assess them
 - Lab and on-the-road experiments
- **Evaluation** of protocol-level Bluetooth threats on recent cars
 - Spoof a trusted smartphone to a car (IVI) using [BIAS](#)+[KNOB](#)
- **Low-cost setup** to reproduce the attacks

Protocol-Level Bluetooth Threats (PLBT)

Automotive Bluetooth

- Modern vehicles support wireless technologies
 - Bluetooth, Wi-Fi, cellular, AM/FM radio, TPMS, ...
- We focus on **Bluetooth**
 - Pervasive, low-power, low-cost
 - By 2024 in 2/3 of all cars ([ref](#))
- Automotive Bluetooth applications
 - Keyless entry system
 - **In-Vehicle Infotainment (IVI)**

Bluetooth In-Vehicle Infotainment (IVI) Unit

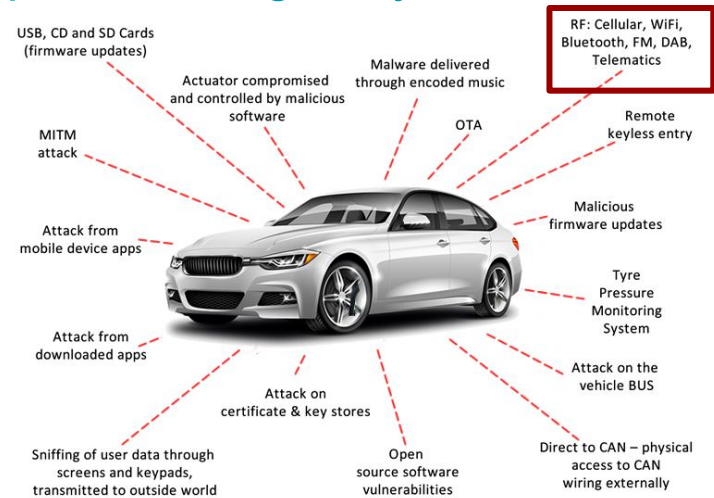


Common Bluetooth Services provided by IVIs

Bluetooth profile	Acronym	Vehicle action
Advanced audio distribution	A2DP	Stream music from a source
Audio/Video remote control	AVRCP	Control music/video player
Hands-free	HFP	Manage calls
Message access	MAP	Read SMS
Object EXchange	OBEX	Send/receive data
PAN Network Encapsulation	BNEP	Join Internet connection
Phone book access	PBA	Read contacts
Serial Port	SPP	Emulate a serial port
SIM access	SAP	Access a SIM card

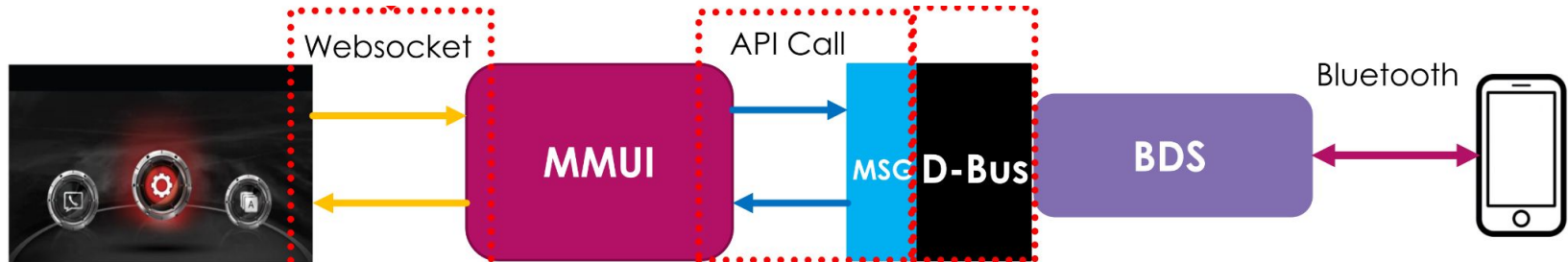
Bluetooth Exposes Vehicles to Wireless Attacks ([ref](#))

- Attacker in wireless range sending malicious packets
 - Safety and security issues for the drivers and the vehicles
 - E.g. [Hackers Remotely Kill a Jeep on the Highway—With Me in It](#)



Implementation-Level Bluetooth Threats (ILBT)

- Exploiting **implementation bugs** in the IVI firmware
 - Buffer overflows, use after free, ...
 - E.g. [Salinas IVI RAT exploiting D-Bus, Bluetooth and SMS](#)
- Mature research area
 - ILBT still present (firmware written in C, no patches, ...)



Protocol-Level Bluetooth Threats (PLBT)

- PLTBs target **vulnerabilities** in the [Bluetooth standard](#)
 - Weak authentication: device spoofing [BIAS\[CVE-2020-10135\]](#)
 - Weak key negotiation: brute-force key [KNOB\[CVE-2019-9506\]](#)
- PLTBs are **unexplored** and **relevant** for automotive
 - Portable across vehicles (car manuf, IVI manuf, SoC manuf, ...)
 - Portable across Bluetooth profiles (infotainment, keyless, ...)
 - Unlike impl-level Bluetooth threats

PLBT Evaluation Methodology

Our Hybrid Methodology (ala [Car Hacking: For Poories](#))

- **Lab** experiments
 - Buy popular IVIs second-hand
 - Power them up in the lab
 - Evaluate them against PLBTs
- **On-the-road** experiments
 - Drive our cars to a safe environment
 - Evaluate them against PLBTs



Lab Experiments Summary

- Bought **five** second-hand IVI (3000 EUR on eBay)
 - Used by KIA, Toyota, Mazda, Nissan, Subaru
- **Power up** the IVI (not easy at it seems)
 - Discard Mazda and Nissan IVIs
- Check IVI **Bluetooth connectivity**
 - Discard Subaru IVI
- **Evaluated** the KIA and Toyota IVIs
 - PLBT, security features, ...

Lab Experiments: IVI Pictures

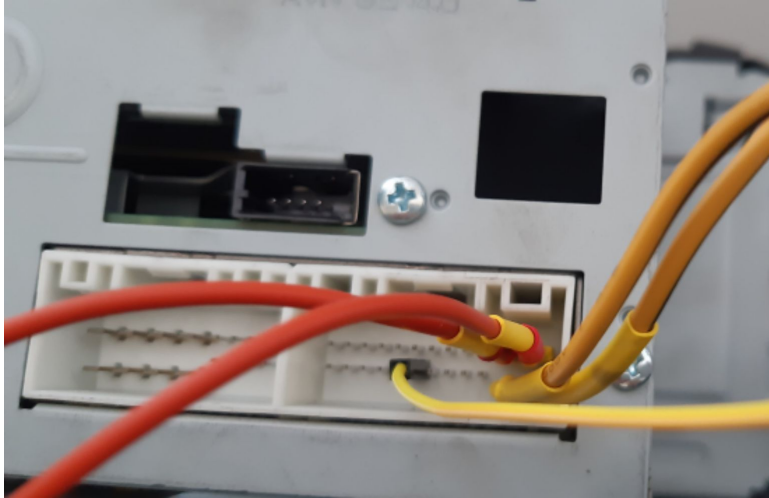


KIA 96560-B2211CA

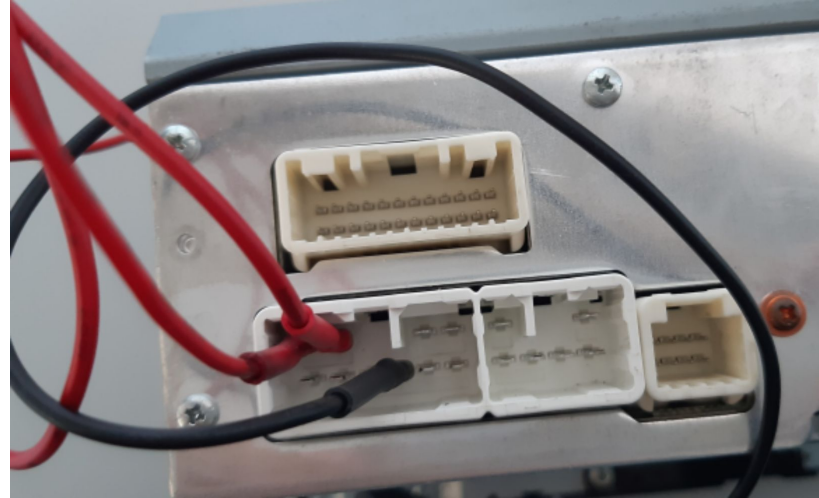


Toyota PT546-00170

Lab Experiments: IVI Power Up (pinout.ru)



KIA 96560-B2211CA
5/24 PIN



Toyota PT546-00170
3/16 PIN

Lab Experiments: IVI Spec

Used by: KIA Soul IVI 2014,
2015

Manuf: Hyundai

Year: 2014

Wireless: Bluetooth and
Wi-Fi

KIA 96560-B2211CA

Sold as: Toyota 86/Cor. IVI
2017, 2018, 2019

Manuf: Toyota

Year: 2012

Wireless: Bluetooth

Toyota PT546-00170

Lab Experiments: IVI Bluetooth® Spec

Manuf: Hyundai

Version: 3.0 (2009)

Chip: not available

Firmware: CSR 8241

Name: KIA MOTORS

Profiles: A2DP, AVRCP,
HFP

KIA 96560-B2211CA

Manuf: Pioneer

Version: 3.0 (2009)

Chip: Qualcomm+Alpine

Firmware: CSR 9079

Name: My Toyota

Profiles: SPP, OBEX,
A2DP, AVRCP, HFP, MAP

Toyota PT546-00170

On the Road Experiments



Suzuki IGNIS'21



Skoda Fabia'20




Skoda Octavia'21

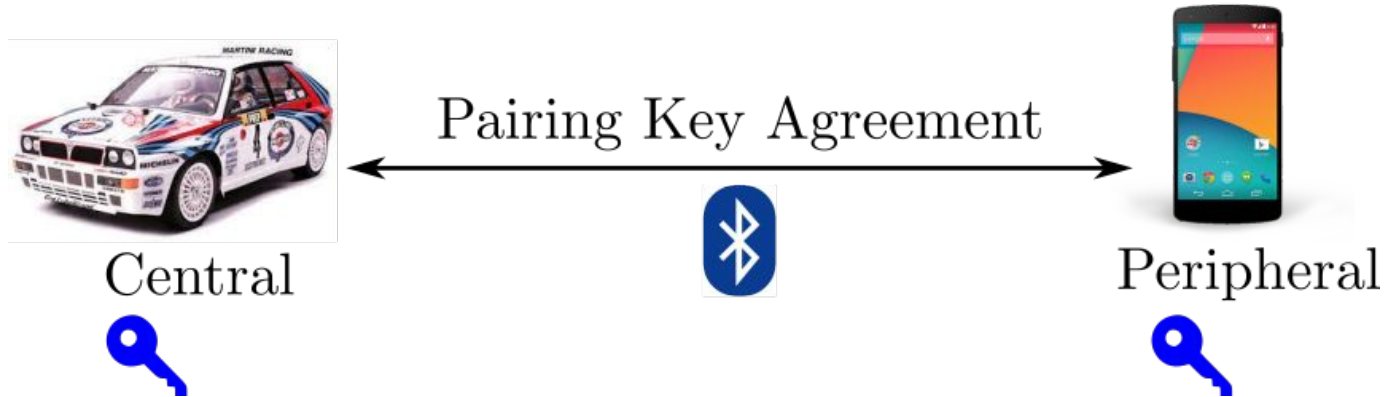
On the Road Experiments: Cars Bluetooth® Specs

	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
Year	2021	2020	2021
BT Manuf.	Harman	Toshiba	Harman
BT Vers.	3.0	4.1	3.0
BT ID	n/a	n/a	n/a
BT Firmw.	CSR 8241	Toshiba 3328	CSR 8241
BT Addr.	Redacted	Redacted	Redacted
BT Name	Suzuki	Skoda BT 1684	Skoda BT
BT Class	0x360408	0x360408	0x360408
BT Profile	SPP, A2DP, AVRCP, HFP, PBA	A2DP, AVRCP, HFP	SPP, MNS, HFM, PBAP, AVRCP, A2DP
Wi-Fi	No	No	No




PLBT Evaluation

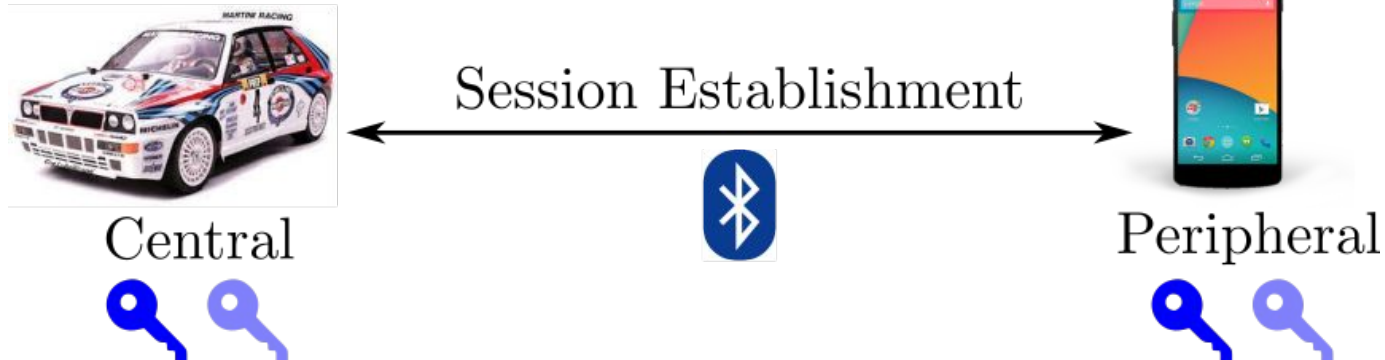
Attack Scenario: Bluetooth Pairing

1. Pair the IVI (car) with a phone
2. Devices generate a long-term pairing key 
3. Accept all permissions and synch data



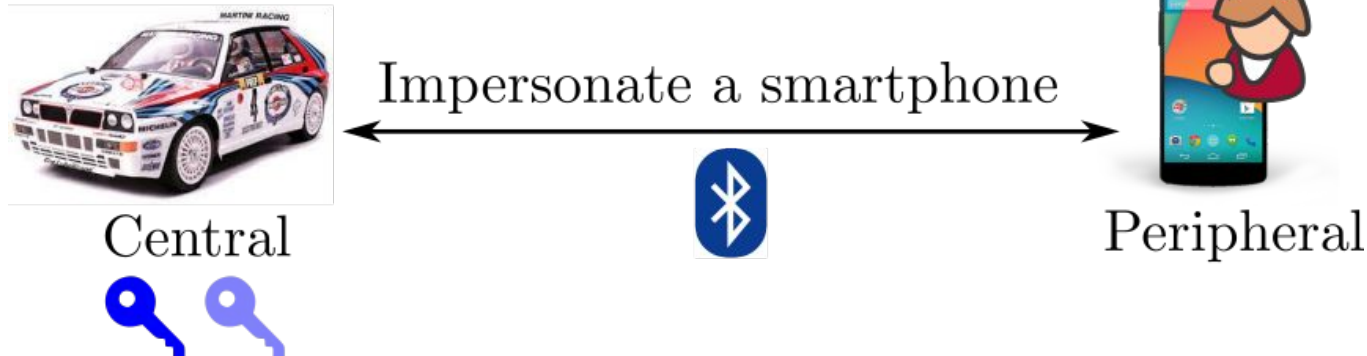
Attack Scenario: Bluetooth Session Establishment

1. Authenticate the pairing key 
2. Negotiate a session key 
3. Encrypt the traffic 
4. Use Bluetooth services (audio, calls, Internet, ...)



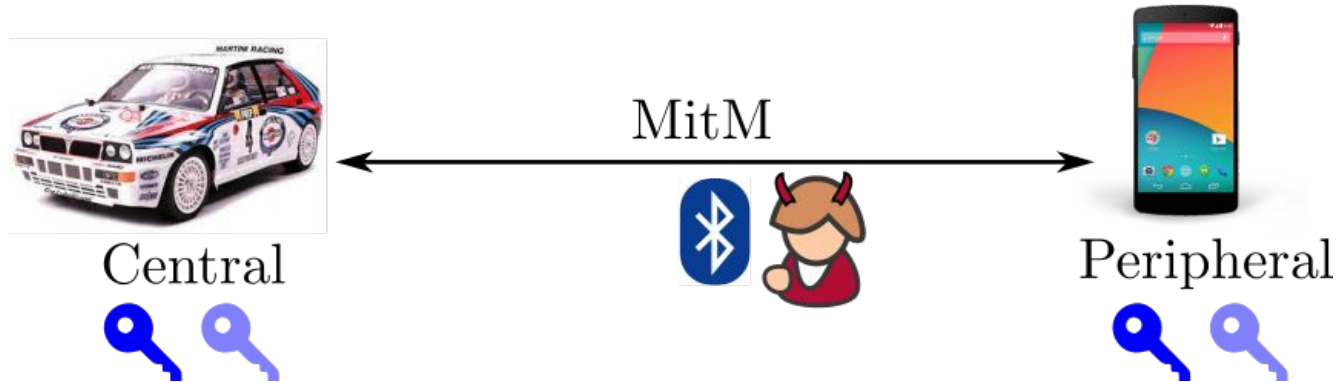
Attack Scenarios: BIAS+KNOB Impersonation Attack

1. Start a session with IVI spoofing the trusted phone
2. Skip pairing key authentication (**BIAS attack**)
3. Negotiate a low entropy session key and brute force it (**KNOB attack**)



Attack Scenarios: BIAS+KNOB MitM Attack

1. Impersonate trusted smartphone to car IVI
2. Impersonate trusted car IVI to smartphone
3. Machine-in-the-middle their connection



Why BIAS+KNOB Impersonation Attack?

- **High impact**

- Portable to all IVIs
- Works against the strongest Bluetooth security mode
- Allow reading sensitive data from the IVI
- Allow sending malicious commands to the IVI

- **Easy to launch, hard to detect**

- No user interaction
- No extra pairing

Why BIAS+KNOB Impersonation Attack? (2)

- **Not tested on vehicles**
 - Tested on IT devices (laptops, smartphones, IoT, ...)
- **Patched in the Bluetooth standard**
 - But what about actual automotive devices?

Eval: 5/5 tested IVIs are **vulnerable to BIAS+KNOB**

	Lab		OtR		
	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Session issues					
Entropy downgrade	1 byte	1 byte	1 byte	1 byte	1 byte
Role switch auth bypass	Yes	Yes	Yes	Yes	Yes
Vulnerable to KNOB & BIAS	Yes	Yes	Yes	Yes	Yes
Pairing issues					
Always Discoverable	No	No	No	Yes	Yes
Always Pairable	Yes	No	No	Yes	Yes
Just Works Downgrade	Yes	Yes	No	Yes	Yes

Eval: 4/5 tested IVIs are **vulnerable to JW Downgrade**

Lab

OtR

	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Session issues					
Entropy downgrade	1 byte	1 byte	1 byte	1 byte	1 byte
Role switch auth bypass	Yes	Yes	Yes	Yes	Yes
Vulnerable to KNOB & BIAS	Yes	Yes	Yes	Yes	Yes
Pairing issues					
Always Discoverable	No	No	No	Yes	Yes
Always Pairable	Yes	No	No	Yes	Yes
Just Works Downgrade	Yes	Yes	No	Yes	Yes

Eval: IVIs **pairing caps are OK**

Lab

OtR

	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Pairing capabilities					
Secure Simple Pairing (SSP)	Yes	Yes	Yes	Yes	Yes
Input Output	Display	Display	Display	Display	Display
Authentication Requirement	AitM	None	AitM	AitM	AitM
Association	Num Comp	Num Comp	Num Comp	Num Comp	Num Comp
Session capabilities					
Secure Connections (SC)	No	No	No	No	No
Unilateral authentication	Yes	Yes	Yes	Yes	Yes
E ₀ cipher (weak)	Yes	Yes	Yes	Yes	Yes

Eval: IVIs **session caps are WEAK**

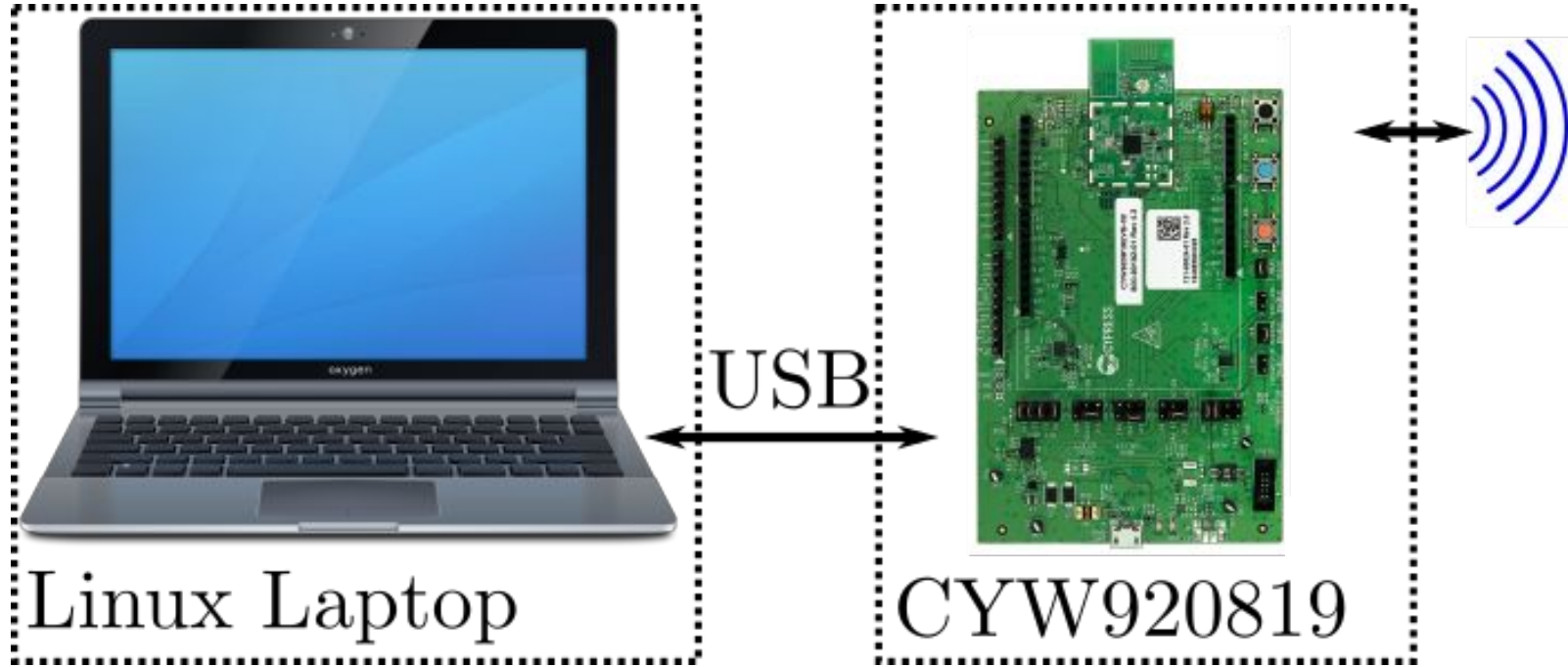
Lab

OtR

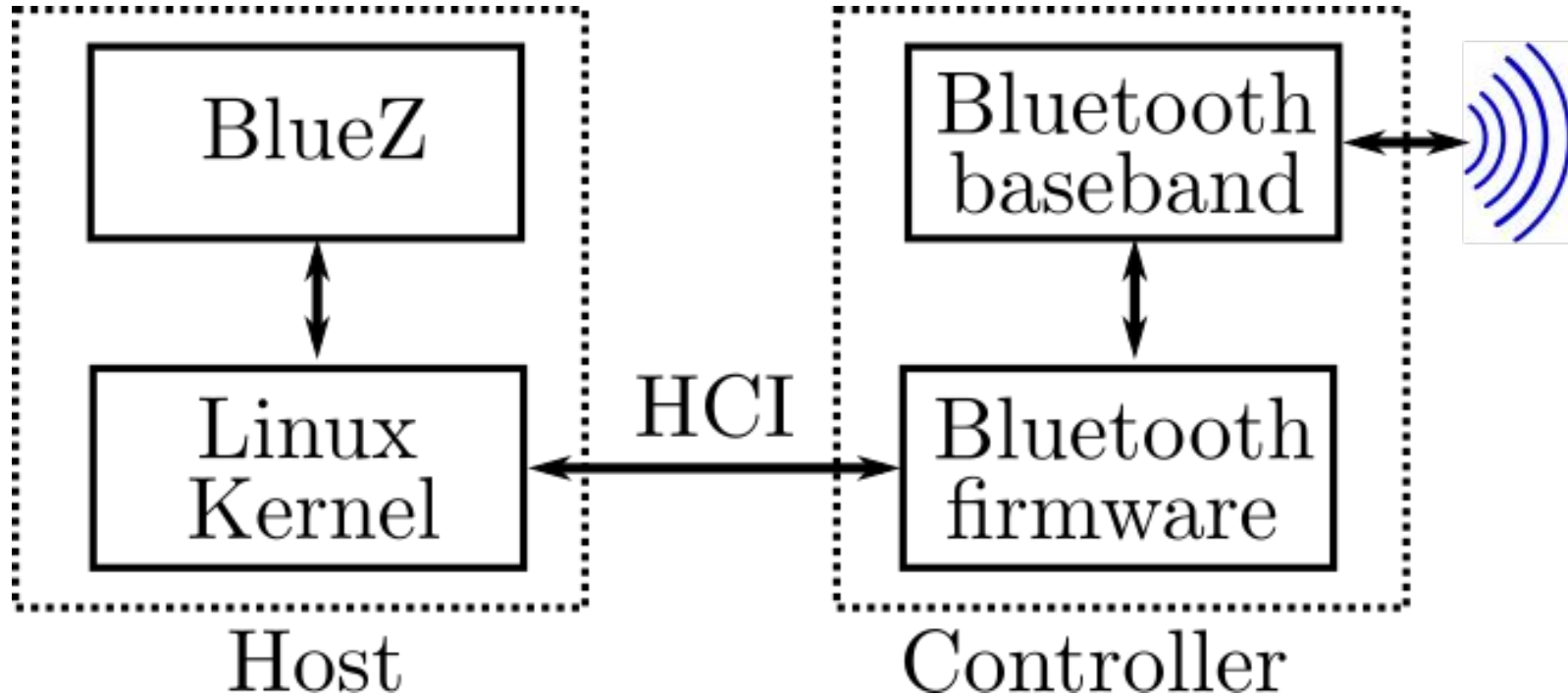
	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Pairing capabilities					
Secure Simple Pairing (SSP)	Yes	Yes	Yes	Yes	Yes
Input Output	Display	Display	Display	Display	Display
Authentication Requirement	AitM	None	AitM	AitM	AitM
Association	Num Comp	Num Comp	Num Comp	Num Comp	Num Comp
Session capabilities					
Secure Connections (SC)	No	No	No	No	No
Unilateral authentication	Yes	Yes	Yes	Yes	Yes
E ₀ cipher (weak)	Yes	Yes	Yes	Yes	Yes

Reproducing the attacks

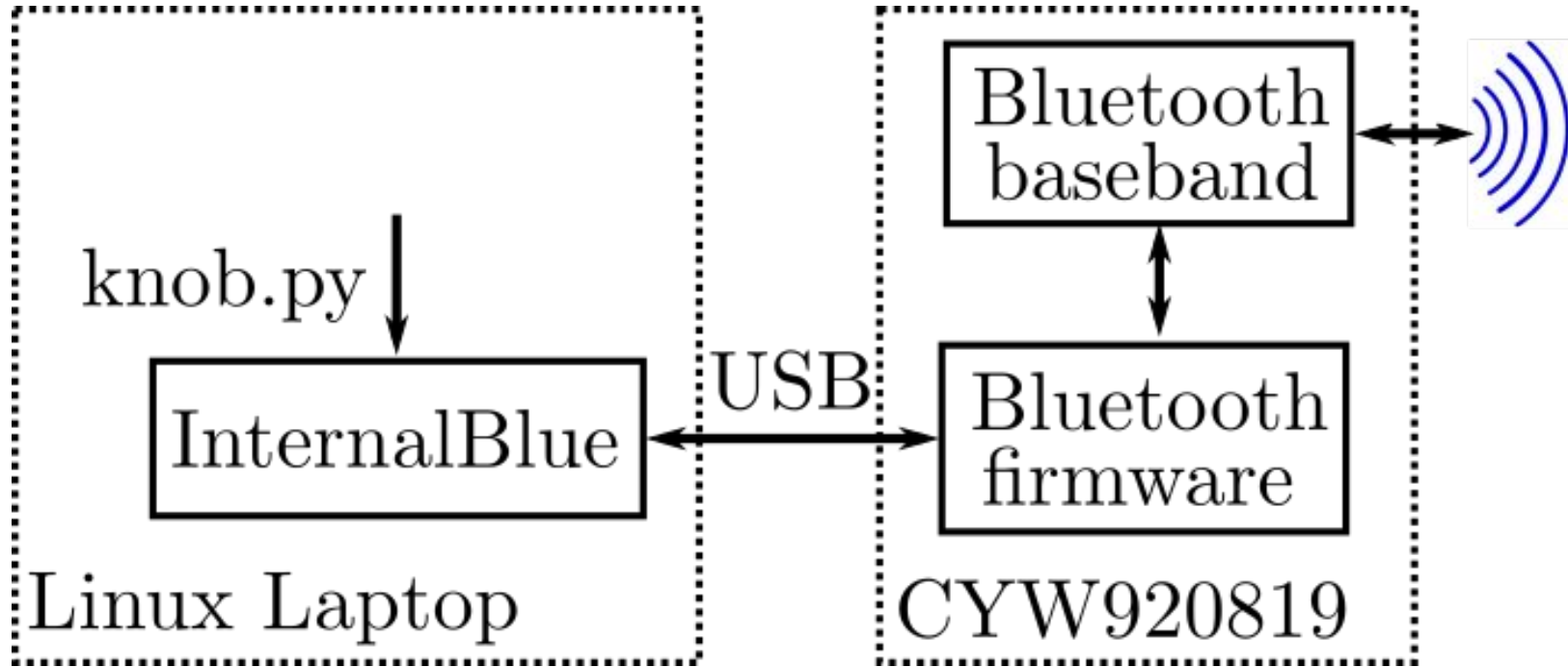
Attack Device



Attack Device: Logic Components



Firmware Dynamic Patching via [InternalBlue](#)



KNOB InternalBlue Patch

```
#!/usr/bin/python2
```

```
# addr RE from firmware
```

```
addr_Lmin = "0x20118a"
```

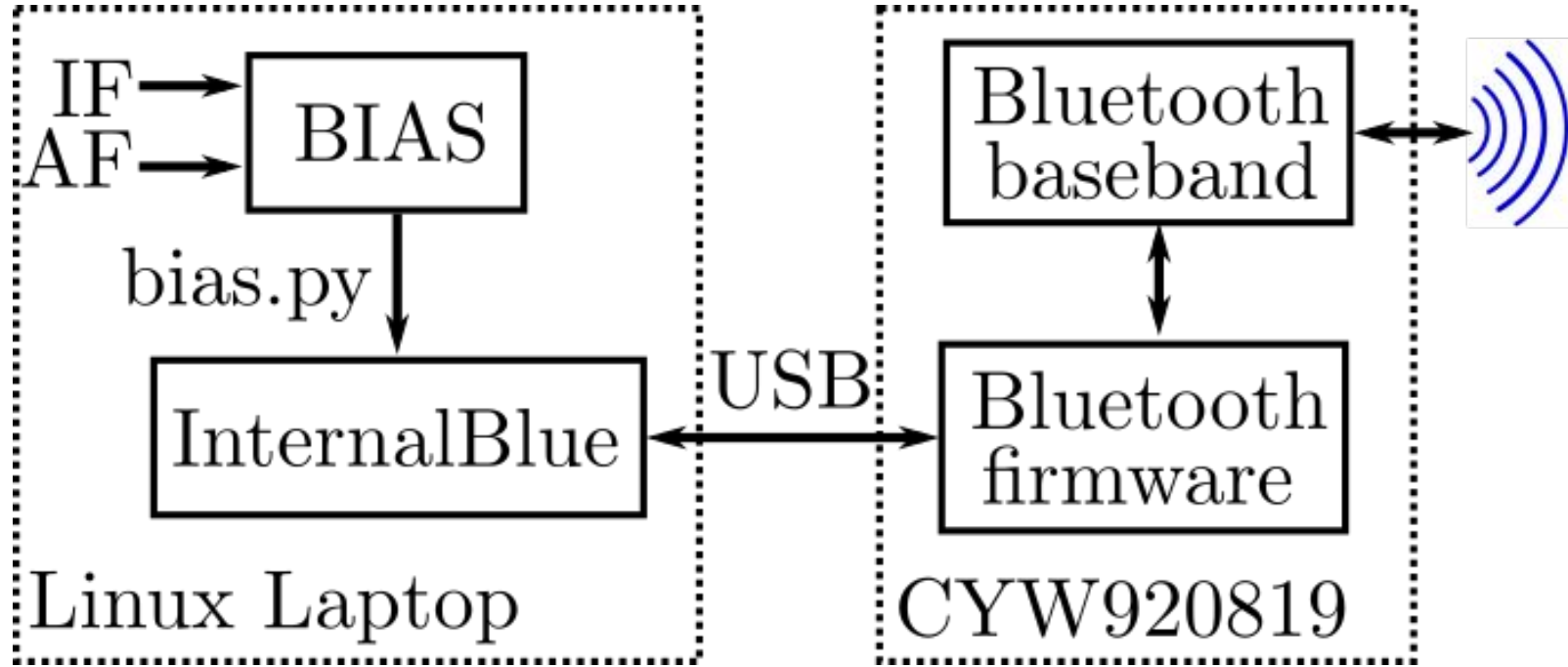
```
addr_Lmax = "0x20118b"
```

```
# 0x1= 1 byte of entropy (KNOB)
```

```
internalblue.writeMem(addr_Lmin, "\0x01")
```

```
internalblue.writeMem(addr_Lmax, "\0x01")
```

BIAS Diagram



BIAS Impersonation File (IF.json)

```
{  
  "if": "X1 7th gen IF.json",  
  "lmin": "07",  
  "lmax": "07",  
  "btadd": "aa:bb:cc:dd:ee:ff",  
  "btname": "BIASing",  
  ...  
}
```

BIAS Attack File (AF.json)

```
{  
  "af": "CYW920819",  
  "arch": "ARM32-le-thumbonly",  
  "hci": "1",  
  "addr_lmin": "0x20118a",  
  "addr_lmax": "0x20118b",  
  "addr_btname": "0x200f48",  
  ...  
}
```

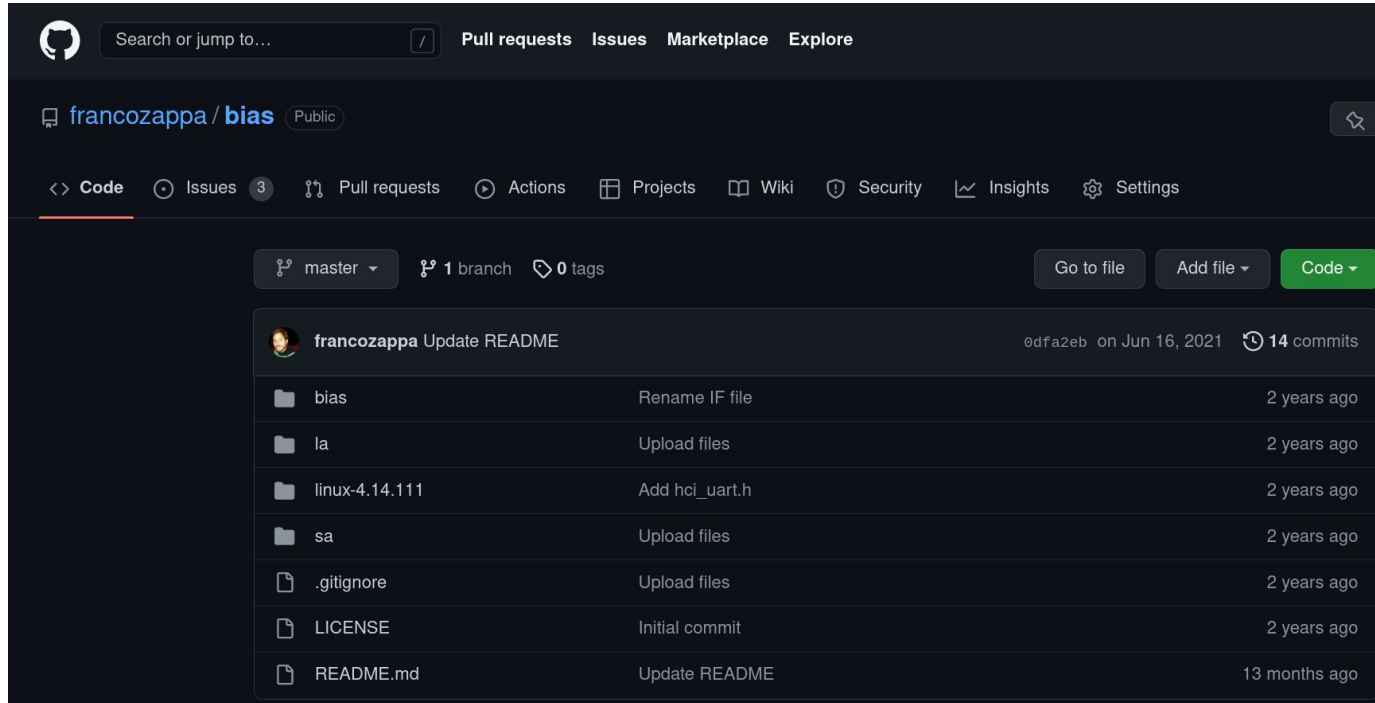
BIAS Template patch1 (bias-template.py)

```
# patch1: always switch to central role
code1 = b" " "
    @Part 1: Make sure we always switch roles
    mov r6, #0x0
    sub sp, #0x18
    add r0, #0xc
    b 0x2e7ad
    " " "
```

...

```
internalblue.patchRom(addrpatch1, patch1)
```

GitHub repository to reproduce the attacks



The screenshot shows the GitHub repository page for **francozappa/bias**. The repository is public and has 14 commits. The commit history is as follows:

Commit	Message	Time
odfa2eb	Update README	13 months ago
	Initial commit	2 years ago
	Upload files	2 years ago
	Update README	2 years ago
	Upload files	2 years ago
	Upload files	2 years ago
	Add hci_uart.h	2 years ago
	Upload files	2 years ago
	Upload files	2 years ago
	Rename IF file	2 years ago

Resources & Acknowledgments

Paper about PLBT Evaluation [woot'22]

On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats

Daniele Antonioli

EURECOM

Biot, France

daniele.antonioli@eurecom.fr

Mathias Payer

EPFL

Lausanne, Switzerland

mathias.payer@nebelwelt.net

Abstract—Cars are some of the most security-critical consumer devices. On the one hand, owners expect rich infotainment features, including audio, hands-free calls, contact management, or navigation through their connected mobile phone. On the other hand, the infotainment unit exposes exploitable wireless attack surfaces. This work evaluates protocol-level Bluetooth threats on vehicles, a critical but unexplored wireless attack surface. These threats are crucial because they are portable across vehicles, and they can achieve impactful goals, such as accessing sensitive data or even taking remote control of the vehicle. Their evaluation is novel as prior work focused on other wireless attack surfaces, notably Bluetooth implementation bugs. Among relevant protocol-level threats, we pick the KNOB and BIAS attacks because they provide the most effective strategy to impersonate arbitrary Bluetooth devices and are not yet evaluated against vehicles.

exploiting the Bluetooth standard, such as attacks on Bluetooth pairing and session establishment. In contrast, prior work on automotive security focused on Bluetooth implementation issues [3], [4], [5], configurations lacking Bluetooth security [6], or security testing methodologies [7]. Hence, our paper fills a research gap in vehicular security, including automotive Bluetooth security.

Protocol-level threats on automotive Bluetooth are not only unexplored but also *relevant*. Vehicles include infotainment units that rely on Bluetooth to exchange data. By attacking those units, an adversary may access sensitive information about the driver, such as contact lists or text messages, along with the ability to send malicious commands to the unit itself. Using a

Paper about KNOB Attacks [sec'19]

The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR

Daniele Antonioli
Singapore University of
Technology and Design
daniele_antonioli@mymail.sutd.edu.sg

Nils Ole Tippenhauer
CISPA Helmholtz Center
for Information Security
tippenhauer@cispa.saarland

Kasper Rasmussen
Department of Computer Science
University of Oxford
kasper.rasmussen@cs.ox.ac.uk

Abstract

We present an attack on the encryption key negotiation protocol of Bluetooth BR/EDR. The attack allows a third party, without knowledge of any secret material (such as link and encryption keys), to make two (or more) victims agree on an encryption key with only 1 byte (8 bits) of entropy. Such low entropy enables the attacker to easily brute force the negotiated encryption keys, decrypt the eavesdropped ciphertext, and inject valid encrypted messages (in real-time). The attack is stealthy because the encryption key negotiation is transparent to the Bluetooth users. The attack is standard-compliant because all Bluetooth BR/EDR versions require to support encryption keys with entropy between 1 and 16 bytes and do not secure the key negotiation protocol. As a result, *the attacker completely breaks Bluetooth BR/EDR security without being detected*. We call our attack **Key Negotiation Of Bluetooth (KNOB)** attack.

The security and privacy of Bluetooth has been attacked and fixed several times, going all the way back to Bluetooth v1.0. [15, 32]. Several successful attacks on the (secure simple) pairing phase [28, 13, 4] have resulted in substantial revisions of the standard. Attacks on Android, iOS, Windows and Linux implementations of Bluetooth were also discussed in [2]. However, little attention has been given to the security of the *encryption key negotiation protocol*, e.g., the Bluetooth security overview in the latest Bluetooth core specification (v5.0) does not mention it [6, p. 240].

The encryption key negotiation protocol is used by two Bluetooth devices to agree on the entropy of the link layer encryption key. Entropy negotiation was introduced in the specification of Bluetooth to cope with international encryption regulations and to facilitate security upgrades [6, p. 1650]. To the best of our knowledge, all versions of the Bluetooth standard (including the latest v5.0 [6]) *require* to use entropy

Paper about BIAS Attacks [sp'20]

BIAS: Bluetooth Impersonation AttackS

Daniele Antonioli
School of Computer and Communication Sciences
EPFL
daniele.antonioli@epfl.ch

Nils Ole Tippenhauer
CISPA Helmholtz Center
for Information Security
tippenhauer@cispa.saarland


Kasper Rasmussen
Department of Computer Science
University of Oxford
kasper.rasmussen@cs.ox.ac.uk

Abstract—Bluetooth (BR/EDR) is a pervasive technology for wireless communication used by billions of devices. The Bluetooth standard includes a *legacy authentication procedure* and a *secure authentication procedure*, allowing devices to authenticate to each other using a long term key. Those procedures are used during pairing and secure connection establishment to prevent impersonation attacks. In this paper, we show that the Bluetooth specification contains vulnerabilities enabling to perform impersonation attacks during secure connection establishment. Such vulnerabilities include the lack of mandatory mutual authentication, overly permissive role switching, and an authentication procedure downgrade. We describe each vulnerability in detail, and we exploit them to design, implement, and evaluate master and slave impersonation attacks on both the legacy authentication procedure and the secure authentication procedure. We refer to our attacks as Bluetooth Impersonation AttackS (BIAS).

subsequent secure connections. Two Bluetooth devices are expected to pair once and securely connect multiple times. During secure connection establishment the devices have to authenticate the possession of the long term key that they have established while pairing.

In a recent paper, researchers showed that Bluetooth secure connection establishment is vulnerable to man-in-the-middle attacks, even if the victims are already paired [4]. In that work however, the attack assumes that there is a legitimate secure connection to break into. The attacker cannot target isolated Bluetooth devices, because the attacker cannot prove possession of the victims' long term key during secure connection establishment.

Acknowledgements

- [Andrea Amico](#) from 
 - Funding, industrial expertise
- Jean-Michel Crepel
 - Helping with the experiments
- [Aurelien Francillon](#)
 - Allowing to test his car



Acknowledgements (2)

- [Nils Ole Tippenhauer](#)
 - Co-author of the KNOB and BIAS papers
- [Kasper Rasmussen](#)
 - Co-author of the KNOB and BIAS papers



Conclusions

- First study of **protocol-level** Bluetooth threats for vehicles
 - Unexplored but relevant attack surface
- Low-cost **methodology** to assess them
 - Lab and on-the-road experiments
- **Evaluation** of protocol-level Bluetooth threats on recent cars
 - Spoof a trusted smartphone to a car (IVI) using [BIAS](#)+[KNOB](#)
- **Low-cost setup** to reproduce the attacks
- Questions? reach out via email or social media