On the Insecurity of Vehicles Against Protocol-Level Bluetooth Threats

IEEE WOOT'22

Daniele Antonioli (EURECOM and EPFL)

Mathias Payer (EPFL)

Contributions

- First study of **protocol-level** Bluetooth threats for vehicles
  - Unexplored attack surface (unlike impl level threats)
- 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
- **Responsibly disclosed** our findings to Auto-ISAC

Automotive Bluetooth

- Modern vehicles support wireless technologies
  - Bluetooth, Wi-Fi, cellular, AM/FM radio, TPMS, …
- We focus on **Bluetooth**
  - Pervasive, low-power, low-cost
  - Will be in ⅔ of all cars by 2024 (ref)
- Automotive Bluetooth applications
  - **In-Vehicle Infotainment (IVI)**
  - Keyless entry system
  - …

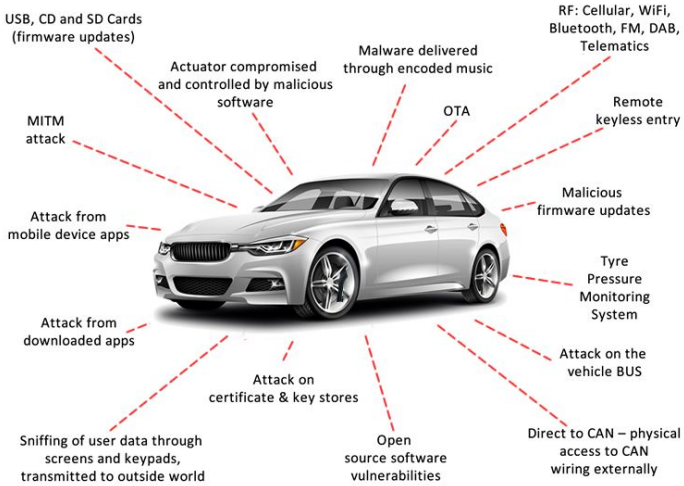
Bluetooth In-Vehicle Infotainment (IVI) Unit

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

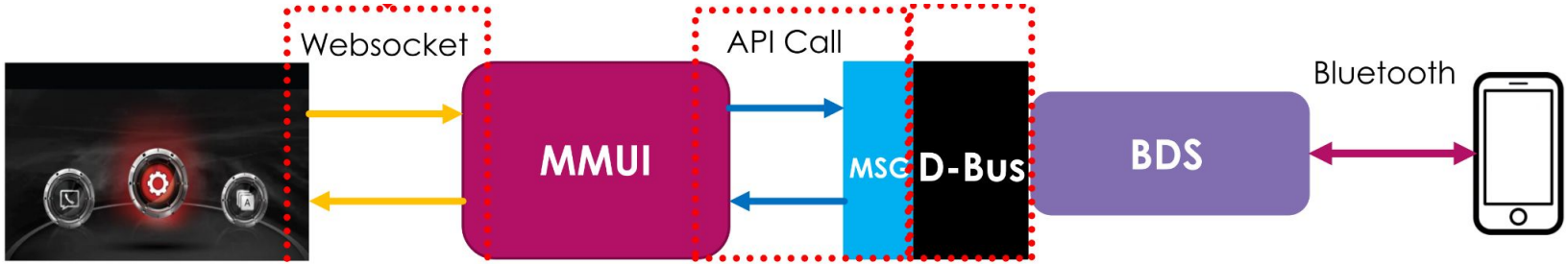
Bluetooth Exposes Vehicles to Wireless Attacks (ref)

- Attacker in wireless range sending malicious packets
  - 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
  - Still present unfortunately (firmware written in C, …)



Protocol-Level Bluetooth Threats (PLBT)

- Target issues in the **Bluetooth standard**
  - Affecting all Bluetooth devices
  - E.g. Bypass session authentication (BIAS, CVE-2020-10135)
  - E.g. Brute-force session keys (KNOB, CVE-2019-9506)
- **Unexplored** and **relevant** for automotive security
  - Threats are portable across vehicles
  - Privacy and safety issues for the driver and the vehicle

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: IVI Pictures

KIA 96560-B2211CA

Toyota PT546-00170

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

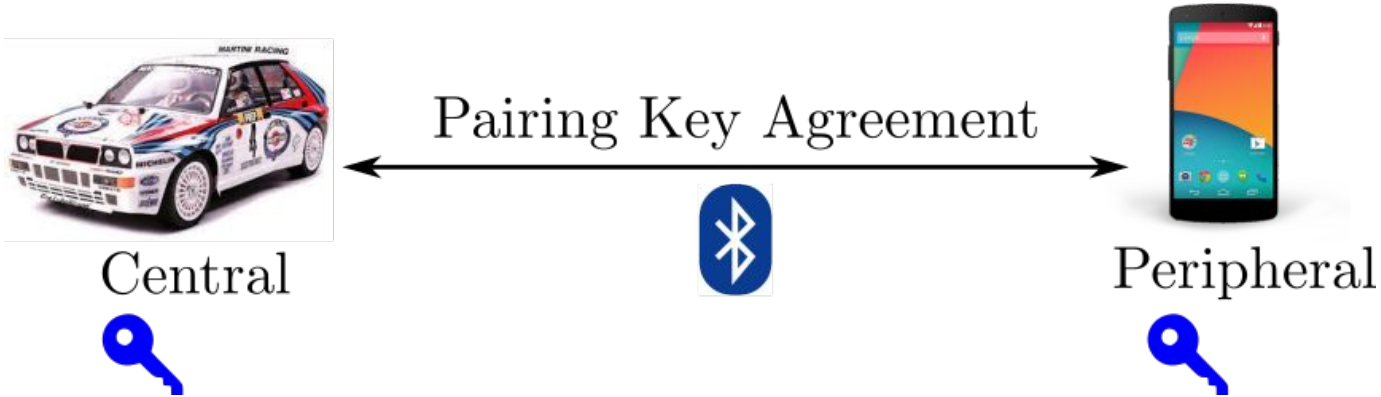
Skoda Octavia’21

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

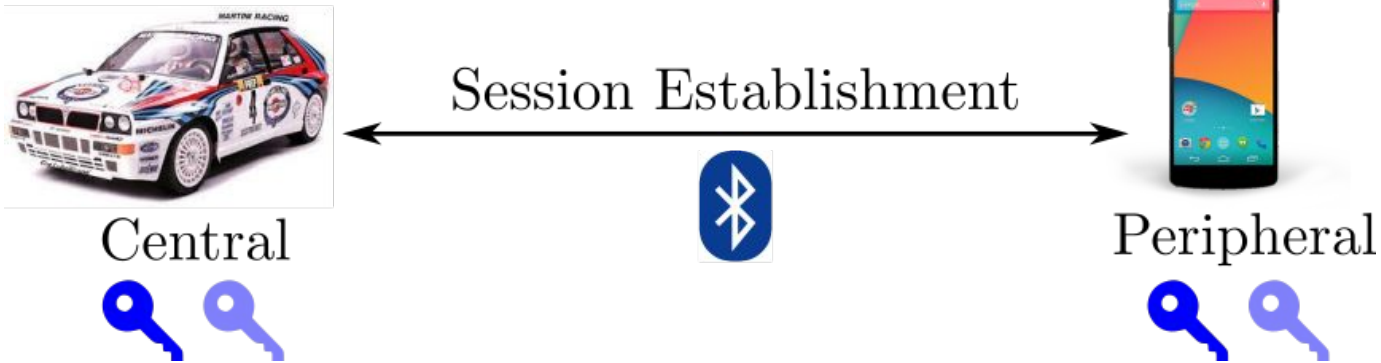
Attack Scenario: Bluetooth Pairing

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



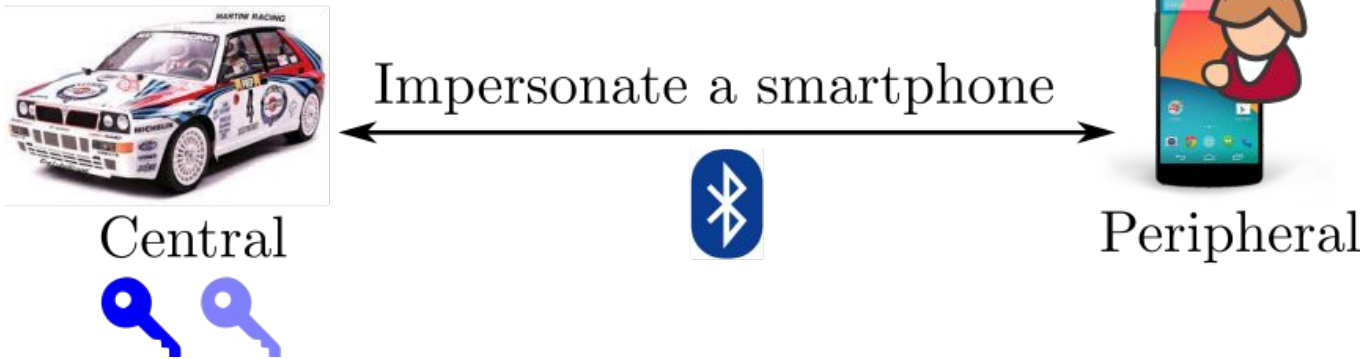
Attack Scenario: Bluetooth Session Establishment

1. Authenticate the pairing key
2. Negotiate a session key
3. Encrypt the traffic



Attack Scenario: 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**)



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: All 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: IVIs pairing caps are OK, **session caps are NOT**

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

Acknowledgements

- Andrea Amico from PRIVACY4CARS
  - 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

Conclusion

- First study of **protocol-level** Bluetooth threats for vehicles
- Low-cost **methodology** to assess them (hybrid lab/otr)
- **Evaluation** of protocol-level Bluetooth threats on recent cars
  - Spoof a trusted smartphone to a car (IVI) using BIAS+KNOB
- **Responsibly disclosed** our findings to Auto-ISAC
- **Links**: paper, code, my website