

Automotive Bluetooth Security



AMUSEC (2025)

[Daniele Antonioli](#)
([EURECOM](#), [S3](#))



Ciao! I am Daniele Antonioli



- Asst. Prof at EURECOM (French riviera, 🌴, 🏠)
 - [Software and System Security \(S3\) group](#)
- Research *applied security and privacy*
 - Protocols (Bluetooth, Wi-Fi, DP3T/GAEN, proprietary, ...)
 - CPS (E-scooters, fitness trackers, EV charging, ICS, IIoT, ...)
 - Tracking (browsers, mobile apps, ...)
 - More at <https://francozappa.github.io>

EURECOM Consortium



EURECOM Location



A Legacy Vehicle

- Hardware and mechanical centric
 - Torque, speed, hp, ...
- Static
 - Leaves the factory with all features
 - Not connected/upgradable (costly recall)
- No security by-design
 - Unprotected CAN bus
 - Vulnerable ECU firmware
 - Trackable TPM



A Software-Defined Vehicle (SDV)

- Software and electronics centric
 - Assisted driving, apps, vision, IVI, ...
- Dynamic
 - Vehicle is a smartphone on wheels
 - Upgradable subsystems
 - Always connected (Cellular, Wi-Fi, BT, ...)
- Some security by design
 - CAN segmentation, automotive ethernet
 - Hardened ECU (secure OS, hypervisor)
 - Security updates



Vehicle Attack Surface is Growing

- Legacy
 - CAN bus
 - ECU firmware
- SDV (includes also legacy)
 - IVI (Android, proprietary OS, ...)
 - Backend (supply chain, upgrade, APIs, ...)
 - Driving (vision, lidar, radar, ...)
 - Connect (keyl, BT, NFC, Wi-Fi, OBD, V2V...)
 - Companion apps (vendor, 3rd party, ...)

Vehicle Attack Surface is Growing (2)

- Huge impacts
 - Confidentiality, integrity, availability, privacy, safety
- Trending vectors (as IT and IoT)
 - Remote (backend, app, telematics, ...)
 - Proximity (Wi-Fi, BT, NFC, ...)
- Affected Industries
 - OEM, Tier-1/2, electric vehicles, fleet management, trains, car sharing, car rental, car dealer, ...

Research paper presented in this talk ([more](#))

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.

Testing vehicles is challenging for several reasons, and we had to design a cost-effective methodology based on hybrid lab/on the road experiments. We evaluated 5 popular infotainment units (e.g., KIA and Toyota units) in the lab and 3 recent cars (e.g., Suzuki and Skoda cars) in a controlled on-the-road environment. We describe our methodology in detail to allow other researchers to reproduce and extend our results. Our Bluetooth protocol-level security evaluation uncovers worrisome facts about the state of vehicular security. For example, all tested devices are vulnerable to BIAS and KNOB, despite the patches in the Bluetooth standard. For example, the standard mandates keys with 7 bytes of entropy, but the tested devices accept keys with 1 byte of entropy. Moreover, all tested devices employ weak and outdated Bluetooth security parameters (e.g., weak authentication protocols and ciphers).

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 protocol-level attack the adversary can impersonate a trusted smartphone to a vehicle infotainment unit over Bluetooth and get arbitrary read and write capabilities. Even worse, since the attack does not depend on the unit's hardware and software details (it exploits a logic Bluetooth bug), the adversary can easily port the attack to other units, even from different vendors.

For our protocol-level Bluetooth security evaluation on vehicles, we selected the BIAS [8] (CVE-2020-10135 [9]) and KNOB [10] (CVE-2019-9506 [11]) attacks. Their combination provides an effective and reliable attack vector to impersonate Bluetooth devices. Moreover, the authors in [10], [8] have *not* evaluated vehicles, so our work extends theirs to an important

Infotainment units (IVI) supports Bluetooth



Common IVI Bluetooth Services

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

IVI Bluetooth Security Research ?

- Implementation Level Bluetooth Threats (ILBT)
 - Mature research area (buffer overflows, use after free, ...)
 - See [Salinas IVI RAT exploiting D-Bus, Bluetooth and SMS](#)
- Protocol Level Bluetooth Threats (PLBT)
 - **Unexplored** and **impactful** (portable attacks)
 - See [KNOB key downgrade](#) and [BIAS impersonation](#)



Bluetooth Security 101

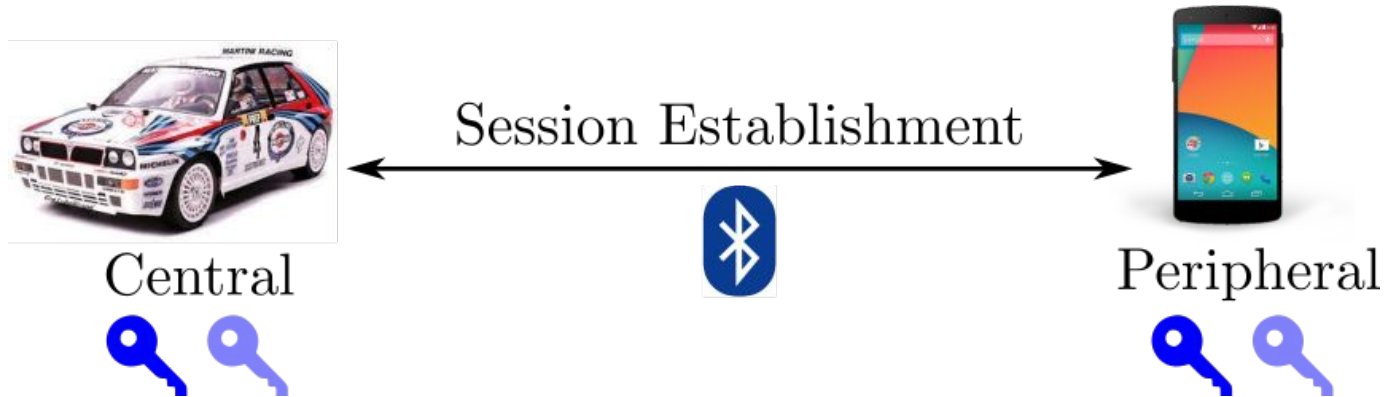
- Roles
 - Central initiates the secure connection (e.g., car)
 - Peripheral respond (e.g., smartphone)
 - Role can be swapped
- **Pairing**
 - Pairing key agreement
 - Opt authenticated with user interaction
- **Session establishment**
 - Session key agreement
 - Session uses authenticated encryption

Automotive Bluetooth Case study

- Focus on **session establishment attacks**
 - Try to impersonate a smartphone to an IVI
 - Try to impersonate an IVI to a smartphone
 - Try to MitM them
- These attacks are **impactful** and **scalable**
 - Can be tested against any IVI
 - Can break confidentiality, integrity, and authenticity

Bluetooth Session Establishment

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



Bluetooth Impersonation Attack

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



Central



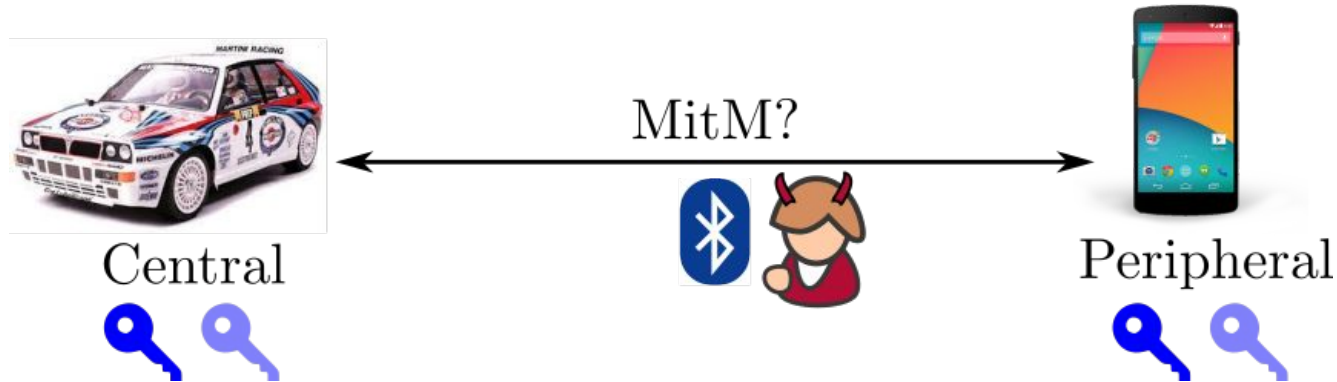
Impersonate a smartphone?



Peripheral

Bluetooth MitM Attack

1. BIAS+KNOB to spoof smartphone to car
2. BIAS+KNOB to spoof car to smartphone
3. Machine-in-the-middle (MitM) their connection



Evaluation setup (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
- Testing equipment
 - power supply, cables, laptop, devboards, ...



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

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

More? Watch the full seminar I gave to ASRG



ASRG 

COMMUNITY SERVICES
AUTOMOTIVE SECURITY

NEW WEBINAR

July 14, 2022

**On the Insecurity of Vehicles
Against Protocol-Level
Bluetooth Threats**



Conclusion. Thanks for your time. Q&A

- Vehicles attack surfaces are growing
- Bluetooth is relatively unexplored and need further research
- Stay tuned because we have a paper under submission about the first large-scale security evaluation of automotive Bluetooth