Bluetooth Security Testing with BlueToolkit: a Large-Scale Automotive Case Study

Vladyslav Zubkov[1] Tommaso Sacchetti[2] Daniele Antonioli[2] Martin Strohmeier[3]

[1]ETH, Switzerland — [2]EURECOM, France — [3]Armasuisse, Switzerland

Published at the 19th USENIX WOOT Conference on Offensive Technologies, 2025

Introduction

Bluetooth is a pervasive wireless technology deployed in billions of devices across automotive, mobile, and Internet of Things (IoT) domains. While many security design and implementation flaws have been uncovered, performing comprehensive testing is challenging and time-consuming because existing exploits are scattered and often non-interoperable.

Contributions

We design and implement BlueToolkit, an extensible, low-cost, black-box Bluetooth Classic security testing framework that automates reconnaissance, exploitation, and reporting. We validate BlueToolkit's effectiveness in the first large-scale systematic evaluation of automotive Bluetooth security, testing 22 vehicles from 14 leading manufacturers. Our evaluation identified 128 vulnerabilities.

The BlueToolkit Framework

BlueToolkit Design

BlueToolkit is a black-box framework that tests Bluetooth targets Over-the-Air (OTA) without requiring knowledge of internal software or hardware. It has three components:

1. **Recon:** collects operational parameters and security configurations.
2. **Execute Exploits:** runs tests from a catalog based on recon data.
3. **Report:** generates machine- and human-readable reports detailing the results.

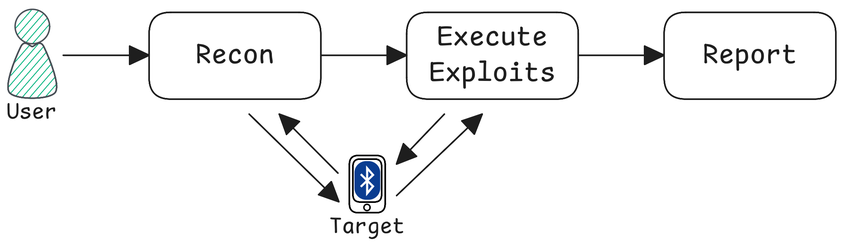

Figure 1: BlueToolkit Stucture.

Novel Attacks

Using BlueToolkit, we identified two authentication bypass implementation flaws (1, 2) and two design-level vulnerabilities (3, 4):

1. **No Numeric Comparison (NC):** certain vehicles automatically accept NC without user interaction, enabling a 0-click MitM position.
2. **JustWorks Central Downgrade:** Some vehicles improperly enforce authentication, rejecting unauthenticated pairing as Initiator (Central) but accepting it as Responder (Peripheral), thus allowing an attacker to downgrade pairing to JustWorks (unauthenticated).
3. **Contacts Extraction:** By impersonating a trusted smartphone, an attacker can leak contacts stored on a vehicle from previous users.
4. **User Account Takeover:** This multi-stage attack chains a MitM position to intercept 2FA SMS codes or emails, allowing an attacker to hijack a victim's online accounts.

Novel Attacks Explained

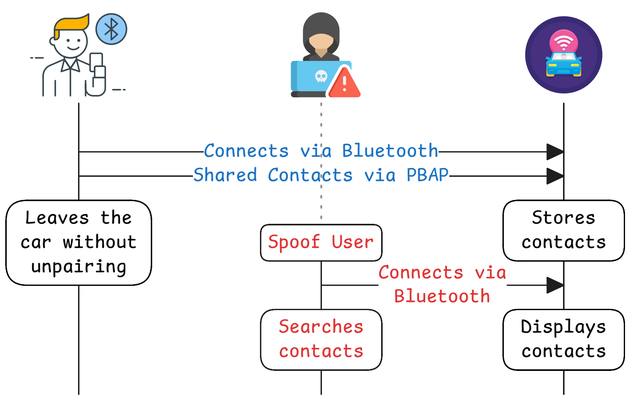

Figure 2: Contacts Extraction Attack

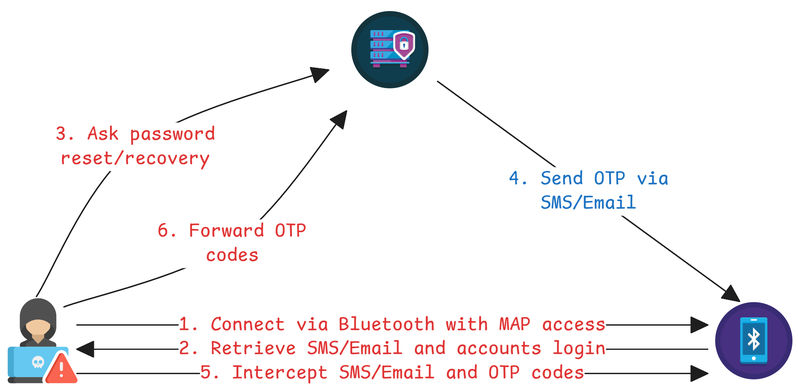

Figure 3: User Account Takeover

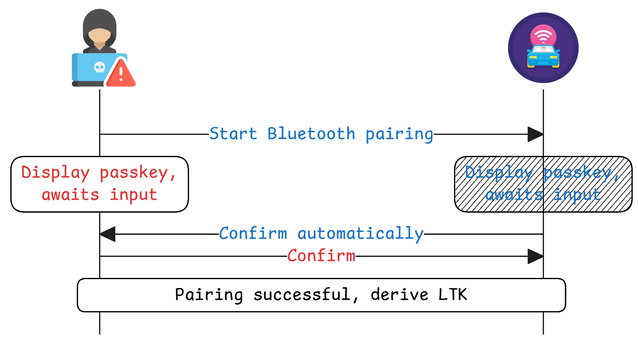

Figure 4: No Numeric Comparison

Tested Vehicles

Findings

- Vehicles often use old Bluetooth versions, with a 7-year average integration delay
- Newer Bluetooth versions do not seem to guarantee better security posture
- 41 vulnerabilities have been acknowledged by manufacturers following our disclosure

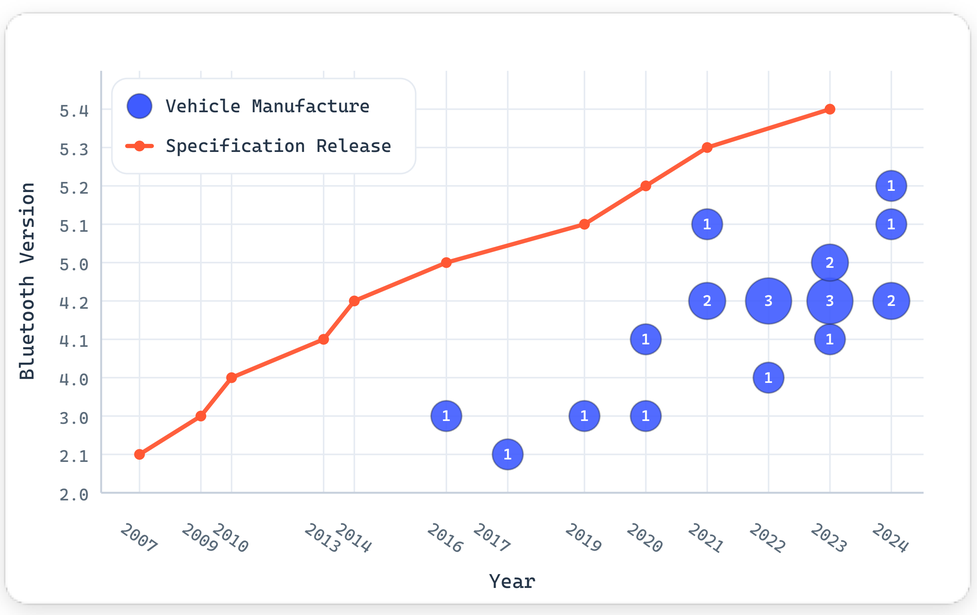

Figure 5: Delay between cars' manufacturing year and their Bluetooth version release

Summary of tested vehicles

Table 1: Results of testing 22 cars with BlueToolkit.

Vehicle	Group	Production	Tests	Positive	Bluetooth	Chipset
Skoda Octavia	VW	2015	8	6	3.0	Marvell
Skoda Octavia	VW	2019	29	3	3.0	Marvell
Skoda Octavia	VW	2022	44	2	4.2	Broadcom
Skoda Enyaq	VW	2023	30	0	4.2	Broadcom
Audi e-tron	VW	2020	44	4	4.2	Broadcom
Audi A5	VW	2020	44	6	4.2	Broadcom
VW T6.1	VW	2022	44	9	4.1	Toshiba
VW ID.3 Pro	VW	2022	44	3	4.2	Broadcom
VW Caddy	VW	2023	44	3	4.2	Cypress
Renault Megane	RNMA	2016	44	10	2.1	Qualcomm
Renault Megane	RNMA	2021	44	13	4.2	Marvell
Renault Zoe	RNMA	2021	44	8	4.2	Marvell
BMW X2	BMW	2021	44	10	4.0	Texas Ins.
Mini Cooper	BMW	2022	44	7	5.0	Texas Ins.
Chevrolet Corvette	GM	2018	44	7	3.0	Qualcomm
Opel Astra	Stellantis	2019	44	6	4.1	Cypress
Honda e	Honda	2020	44	8	5.0	Qualcomm
Sprinter 316CDI	MB	2021	44	4	4.2	Marvell
Hyundai Kona	Hyundai	2022	44	5	5.0	Broadcom
Polestar 2	Geely	2022	32	3	4.2	Qualcomm
Toyota Corolla	Toyota	2023	44	9	5.1	Marvell
Tesla Model Y	Tesla	2023	44	2	5.2	Qualcomm

Work funded by the EU under grant agreement no. 101070008 (ORSHIN) and partially supported by the French ANR under the France 2030 label (NF-HiSec ANR-22-PEFT-0009).