Demo: Bluetooth Impersonation from Pairing Keys Recovered in Used Vehicle Infotainment Systems

Bhargab Acharya
University of Memphis

Christos Papadopoulos
University of Memphis

Spiros Thanasoulas
University of Memphis

Abstract

Used vehicle infotainment head units, routinely sold on secondary markets, retain Bluetooth pairing keys from prior owners alongside personally identifiable information (PII). We demonstrate that an attacker who recovers a BR/EDR link key from such a unit can impersonate the original head unit to a previously paired phone and exercise the Bluetooth profiles the phone had granted to the vehicle—most notably HFP, PBAP, and MAP—to exfiltrate contacts and call logs, intercept calls and SMS-based one-time passwords, and in some configurations invoke the phone's voice assistant, against a locked phone. Co-recovered PII (home address, prior-owner names, GPS traces, paired-device names) makes targeting practical rather than opportunistic. We will demonstrate the full chain live using a salvaged 2016 Honda Pilot head unit against an attacker-controlled test phone.

1 Background and Motivation

Our prior work [1] has shown that used automotive head units retain substantial owner PII, recoverable through a range of forensic techniques, and has characterized the resulting privacy harms in detail. What it did not cover is that the same head units also retain Bluetooth pairing material—specifically BR/EDR link keys—which are not merely artifacts of past use but live credentials. A link key authorizes a specific remote device to re-establish a trusted Bluetooth connection without user interaction. An attacker in possession of one can impersonate the head unit to the previously paired phone, re-entering the trust boundary that the phone established with the vehicle.

Link-key reuse is by design, and key recovery from a physically owned device is unremarkable on its own. What makes the attack practically dangerous is that the same discarded head unit also yields the prior owner's home address, name, contacts, and routine GPS traces. This turns a generic impersonation primitive into a directed attack against a locatable individual whose phone remains paired, in range, and authorized for the profiles the vehicle was granted.

Related work demonstrated at 39C3, reaches a similar impersonation primitive from a different direction [2]: firmware vulnerabilities in Airoha Bluetooth SoCs allow link-key extraction from compromised headphones, which can then impersonate the peripheral to its paired phone. Our setting differs in impact: head units co-store the contextual data that turns generic impersonation into a directed attack, and vehicles are granted broader profiles (PBAP, MAP) than headphones, enabling contact, message, and call-log exfiltration that headphone impersonation cannot achieve.

2 Threat Model

The attacker acquires a discarded head unit (salvage yard, online auction, recycler), and after extracting PII, places him/herself within Bluetooth range of a phone that was previously paired with that unit. The vehicle itself is not required.

Harms to the prior owner. Successful impersonation yields, depending on profile authorizations granted at original pairing time, the phone's contact database, recent call list, and SMS history; the ability to place or answer calls under the owner's number; and interception of incoming SMS, including one-time passwords used for account recovery and 2FA on services such as email, banking, and social accounts. Where the phone permits voice-assistant invocation over Bluetooth from a locked state, the attacker additionally inherits whatever the assistant can do without further authentication. This may include interfacing with a home automation system, for example.

Persistence. The threat persists until the owner unpairs the phone from the head unit. Most users never do this, as evidenced by our ongoing survey of 74 prior owners: 31% took some steps to clear personal data before transfer, but only 16% specifically unpaired their phone from the head unit, indicating that even security-conscious users miss this step absent an explicit prompt. The window is effectively indefinite, bounded only by phone replacement.

3 Generalization Beyond Vehicles

The link-key-as-credential property is not specific to vehicle infotainment systems. Any discarded Bluetooth device that retains BR/EDR pairing material (Bluetooth speakers, headsets, smart-home hubs, fitness equipment) is in principle subject to the same impersonation attack. Vehicle infotainment is a uniquely high-value target: head units co-store the contextual data (names, addresses, routines) needed to convert generic impersonation into directed attacks, and they are durable high-value modules with an active resale market, so their post-ownership trajectory reliably places pairing material in strangers' hands at scale.

4 Attack Chain

Key recovery. On the demo unit (2016 Honda Pilot, Android-based head unit) we obtain a shell over the unit's exposed wireless ADB interface, escalate to root via CVE-2016-5195, and read the pairing database. Link keys co-reside with PII; prior work [1] establishes their recoverability across manufacturers and extraction modalities beyond this demo's specific path. Each entry contains a paired device's Bluetooth address, granted services, BR/EDR link key, and friendly name. The broader feasibility across the used head-unit market—spanning multiple manufacturers, model years 2011–2021, and three distinct extraction modalities—is established in prior work [1], which also reports a field study finding that 35 of 38 used vehicles surveyed at a single dealership retained visible personal data, and 9 of 9 navigation-equipped vehicles retained prior-owner navigation history.

Impersonation. We configure an attacker-controlled Bluetooth host with the recovered BR/EDR address and inject the link key into its pairing store, so that the next connection from the targeted phone completes authentication without re-pairing and without user interaction on the phone.

Profile abuse. Once connected, the attacker exercises the profiles previously authorized for the vehicle. Over **HFP**, AT commands (`AT+CPBR`, `AT+CLCC`, `AT+CNUM`) read the phone book and recent call list and place or answer calls—against a locked phone, without requiring PBAP or MAP. **PBAP**, granted by default in many vehicle pairing flows, yields the full contact database. **MAP**, where enabled, exposes SMS history and incoming messages including OTP codes for account recovery and 2FA. Where the phone permits locked-state voice-assistant invocation over Bluetooth, HFP additionally triggers Siri or Google Assistant.

5 Mitigation

The most effective user-side mitigation is free and straightforward: **unpair the head unit from every paired phone before transfer of ownership**. Factory-resetting the head unit is weaker and unreliable in practice, as resets typically mark storage as free rather than overwriting it. Vendor-side: encrypt the pairing database under a per-unit secret wiped on reset, and tie pairing material to a user profile invalidated on ownership transfer. Phone-side: require re-authorization of PBAP and MAP after prolonged peer absence.

6 Demo Plan

The on-site demo will run the full chain (described above) end to end: power up the salvaged head unit, obtain a root shell over ADB and read the pairing database live (projecting recovered keys and co-located PII with sensitive fields redacted), impersonate the head unit from a laptop to an attacker-owned previously paired phone, dump contacts and call log over HFP and read an SMS OTP over MAP. Code available at https://github.com/bhrg3se/bluetooth_impersonation_demo

7 Future Work

A natural extension is investigating whether the same impersonation attack applies to wireless Android Auto and CarPlay. Both protocols bootstrap over BR/EDR but then establish persistent per-phone state (Wi-Fi credentials, projection-layer keys) that head units retain for seamless reconnection. We plan to characterize what material is stored, whether it is recoverable through the same techniques, and whether it is sufficient to impersonate the head unit at the projection layer. If so, the attacker inherits a far broader capability set than HFP/PBAP/MAP: cross-app messaging, notification mirroring, and navigation control.

8 Ethical Considerations

No component of this demo constitutes an undisclosed vulnerability. Bluetooth link-key impersonation is a known property of the BR/EDR pairing model. The contribution is the end-to-end chain and its practical implications for the used-vehicle parts market, not any single zero-day. Consequently, no coordinated disclosure is in progress for this work.

All phones used in the demo are owned by the authors. The salvaged head unit was purchased on the secondary market; PII recovered from it is not revealed, and is handled per the protocol in our prior work.

References

[1] Acharya, B., Espinoza, D., Thanasoulas, S., Lauzon, S., Balenson, D., and Papadopoulos, C. Persistent personal data exposure across vehicle ownership and control transitions. In *Proceedings of escar USA 2026* (May 2026). To appear.

[2] Steinmetz, F., and Heinze, D. Bluetooth headphone jacking: A key to your phone. Talk at 39th Chaos Communication Congress (39C3), 2025. https://media.ccc.de/v/39c3-bluetooth-headphone-jacking-a-key-to-your-phone.