Artifact Abstract

Security Analysis of LTE Connectivity in Connected Cars: A Case Study of Tesla

Core Idea

Full replication of the experimental tests reported in our work requires significant investment in specialized infrastructure. At the heart of our evaluation is the Amarisoft Callbox Classic [1], a comprehensive cellular test and emulation system. Replication would also require access to test vehicles, including a Tesla Model 3 and Cybertruck, as well as appropriate facilities for safe experimentation, such as a Faraday tent to prevent signal leakage. Due to software licensing agreements with Amarisoft, we are unable to release the exact configuration files used during experimentation. However, our paper provides an extensive methodology in the Appendix that elaborates on the experimental process in detail. Should other researchers have appropriate access to the required equipment, these experimental steps will allow them to reproduce our results in full. With these constraints in mind, we present Wireshark packet captures of control-plane and data-plane traffic captured during experimentation as available artifacts.

Focus of the Artifact

The artifact contains two packet captures collected during experimentation with the Tesla Model 3 and Cybertruck, providing independently inspectable evidence for the LTE control-plane and data-plane observations reported in Section 5. The first capture, `control-plane-attach-example.pcap`, shows a control-plane connection between the vehicle and the Amarisoft LTE network, including the LTE attachment signaling used to support the control-plane analysis. The second capture, `data-plane.pcapng`, shows Internet traffic between the vehicle and online services, including Tesla backend infrastructure, after cellular connectivity had been established. These artifacts are not intended to enable reproduction of the complete wireless experiments, which require access to the vehicles, SDR equipment, programmable SIMs, a controlled LTE core/RAN, and an RF-isolated test environment. Instead, they allow evaluators to verify packet-level observations that support specific empirical claims of the paper. We encourage evaluators to consider this artifact together with Section 3 and Appendix B, which provide the broader experimental context.

Artifact 1: Control-plane signaling trace. The first artifact contains the LTE control-plane signaling generated during vehicle attachment to our controlled LTE network. The trace includes the NAS *Attach Request* and associated LTE/NAS messages exchanged before user-plane communication begins. This artifact supports the "Control-Plane and Parameter Misconfigurations" result and Figure 5. The relevant evidence is located in the *Mobile Station Classmark 2* and *MS Network Capability* fields of the attach procedure. These fields reveal legacy and security-relevant capabilities advertised by the TCU, including backward-compatible cellular features and cipher-suite support. Evaluators can inspect the decoded NAS protocol tree in Wireshark to confirm that the TCU follows a standard attach flow while still exposing legacy capability options that can broaden the attack surface.

Artifact 2: Data-plane backend communication and FBS disruption trace. The second artifact contains user-plane traffic generated after the LTE connection had been established. The capture includes TLS-

[1] https://www.amarisoft.com/

encrypted communication between the vehicle and backend services, followed by faulty traffic near the end of the trace corresponding to the FBS disruption interval. This artifact supports the "False Base Station Susceptibility" result and Figure 4. Because the traffic is encrypted, evaluators should not expect to inspect application payloads. Instead, the relevant evidence is visible through flow metadata, endpoint communication, timing, and TCP behavior. The expected observation is that normal backend communication is present before the attack, while the end of the trace contains retransmissions, stalled flows, or failed communication behavior consistent with cellular disruption. This observation is made from the legitimate network-side node. Near the end of the capture, the legitimate data-plane path no longer receives responsive vehicle traffic, indicating that the FBS attack disrupts the vehicle's ability to maintain backend communication through the legitimate network. This behavior is consistent with our broader FBS experiments, in which the vehicle effectively loses control-plane and data-plane communication with the legitimate network after being coerced toward the rogue cell.

Retrieving the Artifact

The artifact is available at the following location:

Stable DOI:
https://doi.org/10.5281/zenodo.19699792

Tools required for evaluation: Wireshark v4.4.6

What the Evaluation Should Check

This section describes the concrete checks that evaluators can perform on the two packet captures. In particular, evaluators should confirm that the first trace contains LTE control-plane signaling with the capability fields discussed in Figure 5, and that the second trace contains encrypted backend communication followed by transport-layer failure behavior consistent with the FBS disruption described in Figure 4.

1. **`control-plane-attach-example.pcap`: LTE control-plane signaling and capability exposure**

   This capture should be opened in Wireshark and inspected using the LTE-related protocol dissectors. Depending on the capture point and Wireshark version, the relevant messages may appear as NAS-EPS messages (encapsulated inside S1AP), or as LTE RRC messages carrying NAS payloads. If Wireshark does not automatically decode the trace, evaluators may need to use *Analyze* → *Decode As* and decode the relevant transport as S1AP, LTE RRC, and NAS-EPS, depending on the visible encapsulation. Please visit `https://docs.srsran.com/projects/4g/en/rfsoc/general/source/5_troubleshooting.html` for further information about decoding under the Section "Examining PCAPs with Wireshark".

   If the trace uses S1AP encapsulation, the *LTE Attach Request* is typically visible inside an *Initial UE Message* or an uplink NAS transport message. If the trace exposes LTE RRC directly, the attach request may be carried inside an *RRCConnectionSetupComplete* message as a NAS PDU. Evaluators should not require both views to be present. The important check is that the *NAS Attach Request* can be decoded and inspected.

   The expected checks are as follows:

(a) **Verify that the trace contains an LTE attach procedure.** Evaluators should locate the beginning of the vehicle attachment attempt and identify the *NAS Attach Request*. The relevant frame number is 4. The approximate timestamp is 0.045994. The expected message type is:

```
NAS EPS Mobility Management Message: Attach request
```

(b) **Inspect the *Mobile Station Classmark 2* field.** In the decoded *NAS Attach Request*, evaluators should expand the relevant capability fields and locate:

```
Mobile Station Classmark 2
```

This field is one of the fields used in Figure 5. Evaluators should verify that it is present and decoded by Wireshark. The expected observation is that the TCU advertises legacy radio capability information as part of the normal attach procedure. The exact frame containing this field is frame 4. Relevant decoded subfields include legacy GSM-class capability information and ciphering-related capability flags, including the advertised support for A5-family ciphering such as A5/3 where shown by the Wireshark decoder.

(c) **Inspect the *MS Network Capability* field.** Evaluators should also locate and expand:

```
MS Network Capability
```

This is the second field used in Figure 5. The expected observation is that the TCU advertises backward-compatible network capabilities, including support for legacy cellular mechanisms. Relevant decoded subfields include GPRS/GERAN-related network capability flags, GEA-family ciphering support such as GEA2 and GEA3 where decoded, and mobile-terminated point-to-point SMS support over legacy signaling paths. These fields support the paper's claim that the TCU exposes backward-compatible cellular capabilities during attachment.

(d) **Inspect the LTE security capability information.** Evaluators should inspect the UE/EPS network capability fields associated with LTE ciphering and integrity support. The expected observation is that the TCU advertises support for LTE encryption and integrity algorithms. In particular, evaluators should record whether the trace shows support for:

```
EEA0 / 128-EEA1 / 128-EEA2 / 128-EEA3
EIA0 / 128-EIA1 / 128-EIA2 / 128-EIA3
```

The paper reports that the TCU supports null ciphering, i.e., EEA0, alongside stronger LTE ciphering algorithms, while null integrity is not accepted during security mode negotiation (i.e., it should be 0). Evaluators can verify the advertised capability values visible in the trace and compare them with the discussion in Section 5.

(e) **Confirm that the attach flow is standards-like.** The artifact should not be interpreted as showing malformed or proprietary Tesla signaling. Instead, evaluators should observe a conventional LTE attach flow with standard NAS/RRC/S1AP/MAC/RLC message structures. Depending on the capture, the sequence may include NAS messages such as:

```
Attach Request
```

```
Idenity Request / Identity Response
Authentication Request / Authentication Response
Security Mode Command / Security Mode Complete
UE Capability Enquiry / UE Capability Information
```

The exact sequence may vary depending on capture point and filtering. The important observation is that the capability exposure occurs during a normal LTE attachment procedure.

2. **`data-plane.pcapng`: Backend communication and FBS-induced disruption**

This capture should be opened in Wireshark and inspected as an IP/TCP/TLS data-plane trace. Unlike the first artifact, this trace is not intended to expose LTE NAS or RRC signaling. Instead, it shows user-plane communication after LTE connectivity had already been established. The main purpose is to verify that the vehicle was actively communicating with backend services and that, near the end of the trace, the communication becomes faulty in a manner consistent with the FBS disruption interval.

The expected checks are as follows:

(a) **Verify that the trace contains user-plane IP traffic.** Evaluators should first confirm that the capture contains IP/TCP traffic associated with the vehicle's data connection. The vehicle-side IP address is 192.168.3.2 (given during the PDU Session Establishment in the control-plane). The legitimate network-side capture point is 192.168.3.1, which can be seen in the ICMP traffic.

(b) **Verify that backend communication is present before the disruption.** In the earlier portion of the trace, evaluators should observe normal bidirectional communication between the vehicle and external services. This may include DNS lookups, TCP three-way handshakes, TLS handshakes, QUIC and TLS application data. Relevant filters include:

```
dns
quic
tls.handshake
tls.record
tcp.stream eq [stream_number]
ip.addr == 192.168.3.2
```

The expected observation is that the vehicle has established data-plane connectivity and is exchanging traffic with online services.

(c) **Locate the transition from normal traffic to faulty traffic.** Another key point of the data-plane artifact is the change in behavior near the end of the trace. The approximate attack/disruption interval begins at:

```
Frame: 5694 (QUIC)
Time:  787.936355898
```

and continues until:

```
Frame: 5768 (ICMP)
Time:  1885.773990854
```

(d) **Verify retransmissions or failed transport behavior near the end of the trace.**
Evaluators should inspect the end of the capture from the legitimate network-side node and verify that the data-plane path no longer receives responsive vehicle traffic. The expected observation is a transition from normal backend communication to failed or one-sided communication during the FBS disruption interval. In particular, evaluators should observe unanswered ICMP echo requests, repeated TCP retransmissions, stalled TLS/TCP streams, failed connection attempts, and one-directional QUIC traffic from the server side. The unanswered ICMP traffic is especially useful because it indicates that the UE is no longer reachable through the established PDU session with the LTE core.

This artifact should be interpreted as evidence of availability disruption, not confidentiality compromise or payload manipulation. Since most application traffic is encrypted, evaluators should not expect to verify plaintext vehicle telemetry, backend commands, or application semantics. The relevant observation is that successful bidirectional backend communication is present before the FBS disruption, while the legitimate network path later exhibits failed transport behavior consistent with cellular disruptions.