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

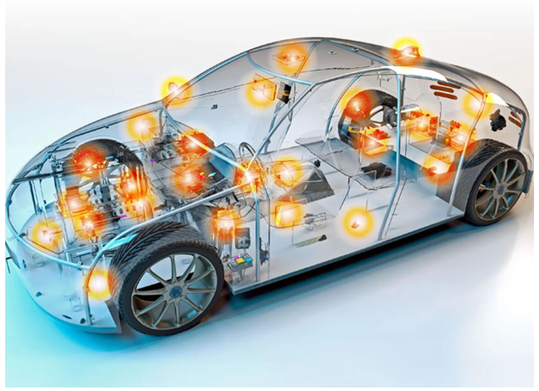
Evangelos Bitsikas, Jason Veara, Aanjhan Ranganathan

Northeastern University

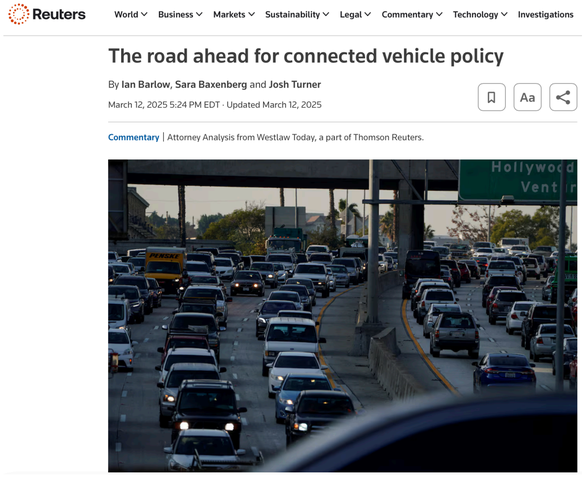
20th USENIX WOOT Conference on Offensive Technologies (WOOT'26)
Baltimore, MD, USA

Vehicles Today

- Up to **150 electronic control units** and approximately **100 million lines of software**
- Connected through **cellular networks, Wi-Fi, Bluetooth, mobile apps, and cloud services**
- Connectivity enables **remote control, navigation, diagnostics, telemetry, and software updates**
- The vehicle's external interfaces create a **remote attack surface** with implications for privacy, availability, and safety



The Car in the Age of Connectivity: Enabling Car to Cloud Connectivity, IEEE Spectrum



Reuters

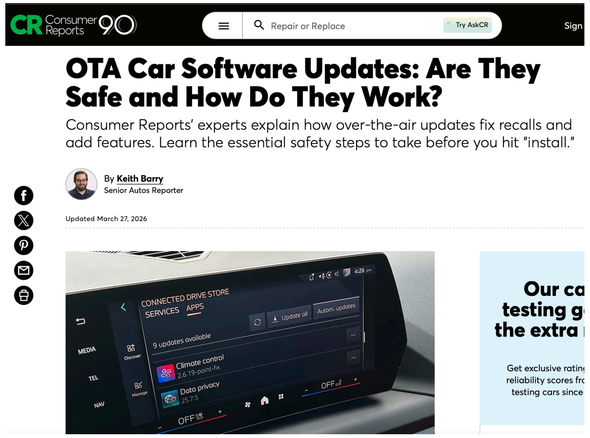
World Business Markets Sustainability Legal Commentary Technology Investigations

The road ahead for connected vehicle policy

By **Ian Barlow, Sara Baxenberg** and **Josh Turner**

March 12, 2025 5:24 PM EDT · Updated March 12, 2025

Commentary | Attorney Analysis from Westlaw Today, a part of Thomson Reuters.



CR Consumer Reports

Repair or Replace

Try AskCR

Sign

OTA Car Software Updates: Are They Safe and How Do They Work?

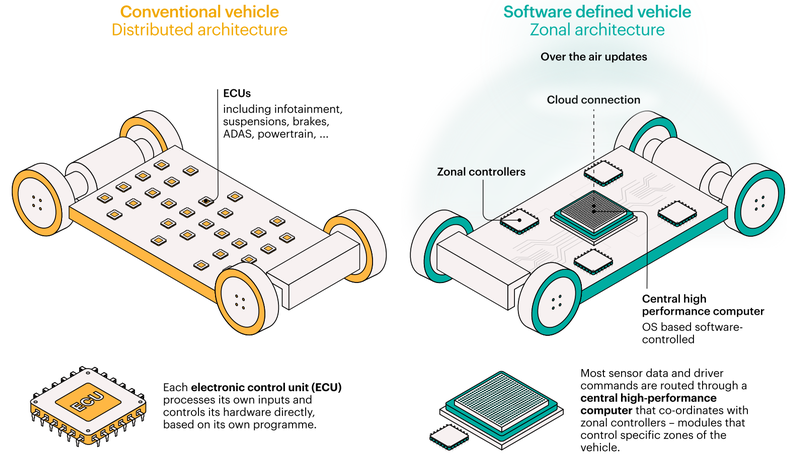
Consumer Reports' experts explain how over-the-air updates fix recalls and add features. Learn the essential safety steps to take before you hit "install."

By **Keith Barry**
Senior Autos Reporter

Updated March 27, 2026

Our ca
testing g
the extra

Get exclusive ratin
reliability scores fr
testing cars since



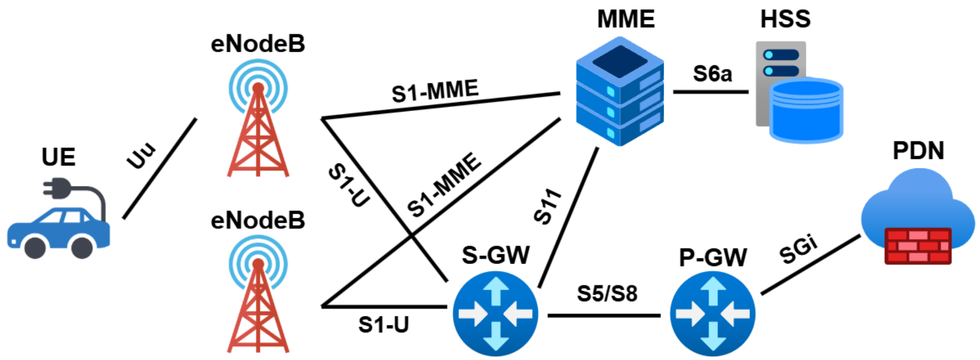
Vehicle Software and Software-Defined Vehicles, International Energy Agency

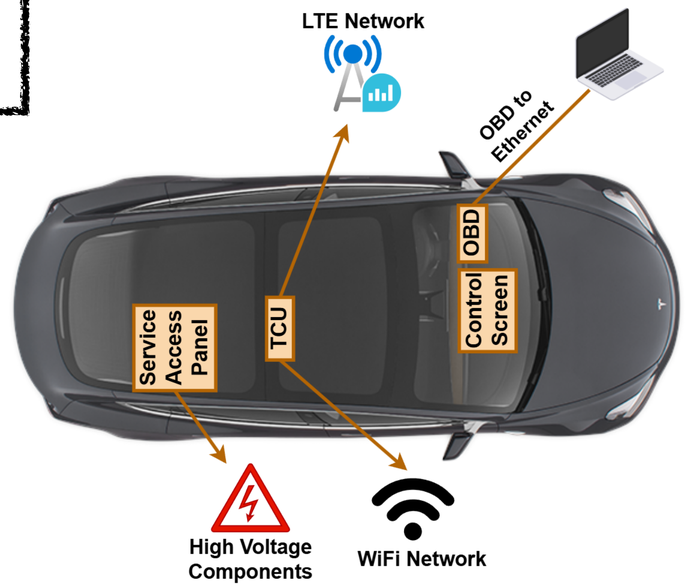
What are connected vehicles?

Vehicles that:

- Include an embedded **cellular modem**, typically within a Telematics Control Unit
- Integrate cellular connectivity with the vehicle's software and electronic systems
- Can register with and communicate through commercial mobile operators
- Use **SIM or eSIM credentials** for network authentication
- Exchange data with OEM backends, cloud services, mobile applications, and external infrastructure

They use cellular connectivity to establish a persistent communication channel between the vehicle and the outside world.





Cellular Testing So Far

Various Categories:

- Formal protocol analysis
- Specification-driven testing
- Over-the-Air testing of COTS UEs
- Baseband implementation testing
- And so on …

"LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE"
Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino
Network and Distributed System Security Symposium (NDSS), 2018.

"DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices"
CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim
31st USENIX Security Symposium (USENIX Security '22), 2022.

"FirmWire: Transparent Dynamic Analysis for Cellular Baseband Firmware"
Grant Hernandez, Marius Muench, Dominik Maier, Alyssa Milburn, Shinjo Park, Tobias Scharnowski, Tyler Tucker, Patrick Traynor, and Kevin Butler
Network and Distributed System Security Symposium (NDSS), 2022.

"UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework"
Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, and Christina Pöpper
16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), 2023.

Why it may not be enough:

- Device characteristics
- Context-Environment
- Different abstraction levels
- Limited control
- Additional services
- Stricter constraints & additional standards

We ask not only whether the modem or protocol is vulnerable, but how adversarial cellular behavior manifests at the vehicle-system level.



Motivation

Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26

How are production vehicle LTE/5G stacks impacted by **cellular-level attacks** and **misconfigurations**, which **vehicle-specific functions** are affected, and what **safety/regulatory implications** arise?

Why?

Vehicles are first-class cellular endpoints

Telematics systems remain opaque and under-tested

Their connectivity model differs from smartphones

Cellular failures may affect critical and safety-relevant services

Automotive cellular risks are insufficiently characterized

Prior work mainly focuses on smartphones and generic UEs

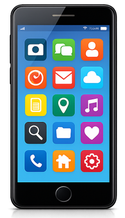
Differences with Smartphones

Same cellular protocols—very different operational context

- Persistent and often unattended cellular endpoint
- OEM-provisioned and controlled connectivity
- Limited user visibility, control, and diagnostics
- Closed and difficult-to-inspect telematic stacks
- Support for remote, diagnostic, OTA, and emergency-related services
- Broad and changing mobility environment
- Greater operational and potentially safety-relevant consequences



VS

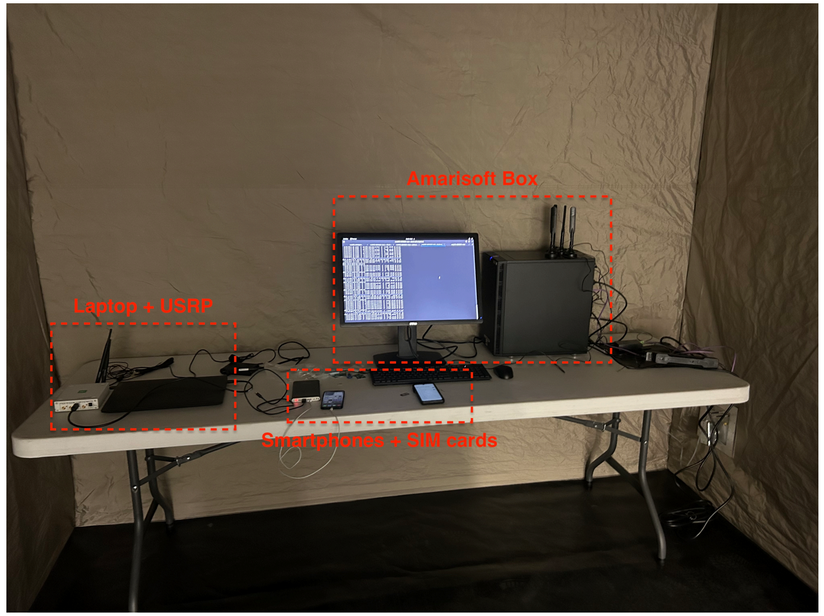


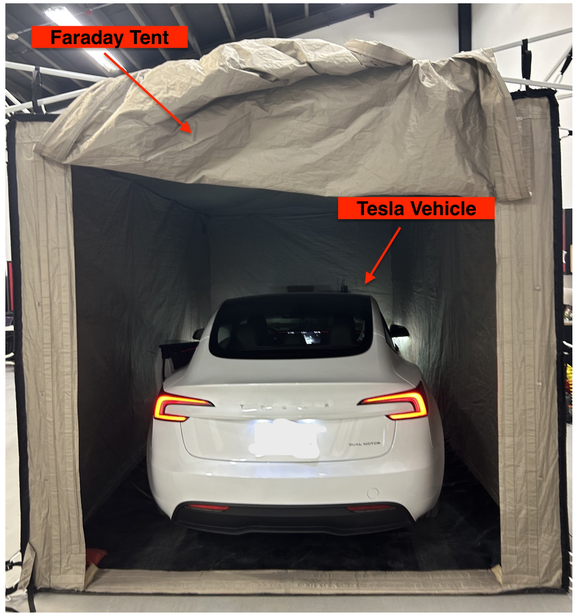
Harder for security and research!

Experimental Setup

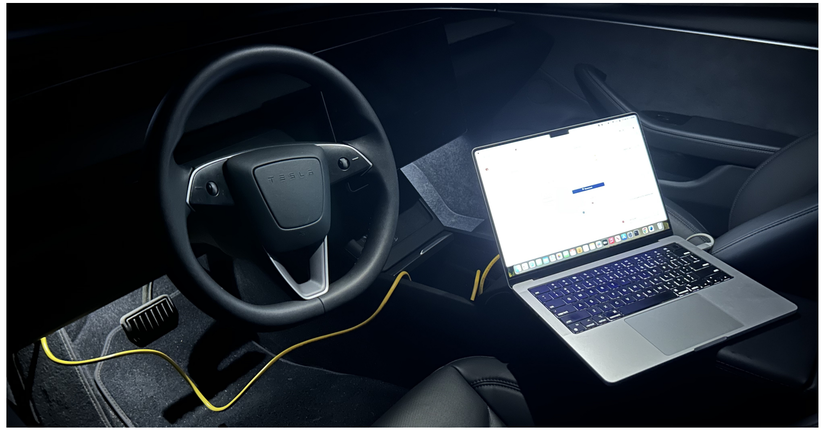
Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26





Consumer Reports in Connecticut*





Why Tesla?

Most configurable vehicle

Allows physical SIM cards

Connectivity dependent

* https://www.consumerreports.org/cars/

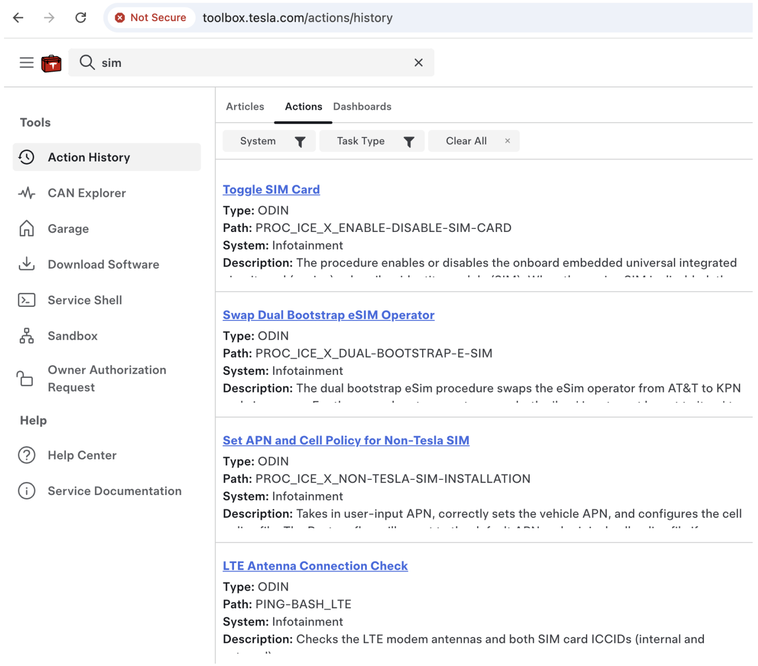
Methodology

Northeastern University
Khoury College of Computer and Information Sciences

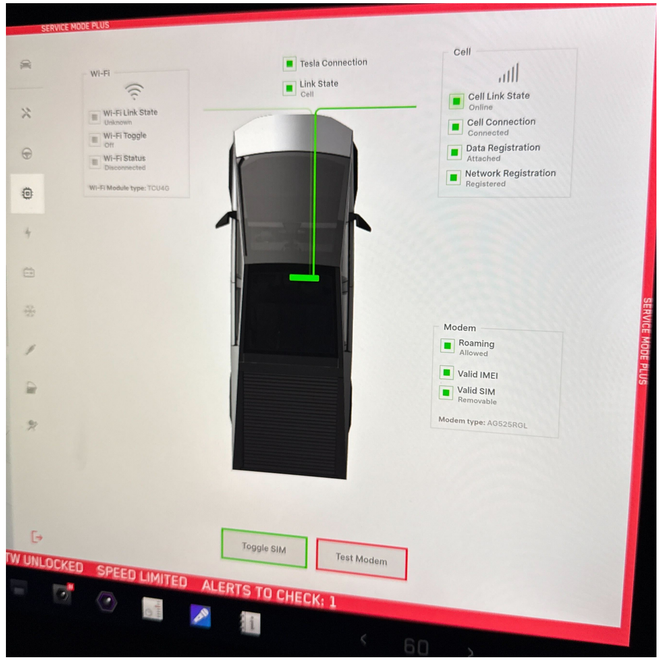
WOOT '26

1. *Assemble the necessary HW and SW*
2. *Figure out how to connect it to a custom setup* (e.g., supported operators to mimic, proper PLMN configurations, Tesla connectivity functions)
3. *Perform the security testing*
4. *Collect and evaluate the results*

Dedicated methodology for vehicle integration!







Testing Categories & Threat Model

Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26

Main Tests

IMSI Catching susceptibility

False Base Station susceptibility

Emergency broadcast spoofing

Rogue-PLMN registrations

Fault injection for fallback behavior analysis

Extra Tests

APN validations

Roaming & whitelisting bypass

Legacy service support (GSM/SMS)

Data-Plane disruptions (via DoS)

Not an exhaustive assessment!

Threat Model

Wireless Adversary ONLY

Passive observer & active transceiver

No access to software, hardware or credentials



Physical Access for:
(1) Integration to custom setup
(2) Deep Investigation of Processes

Ethics

Controlled, RF-isolated Environment

Strictly non-invasive testing (Black-box)

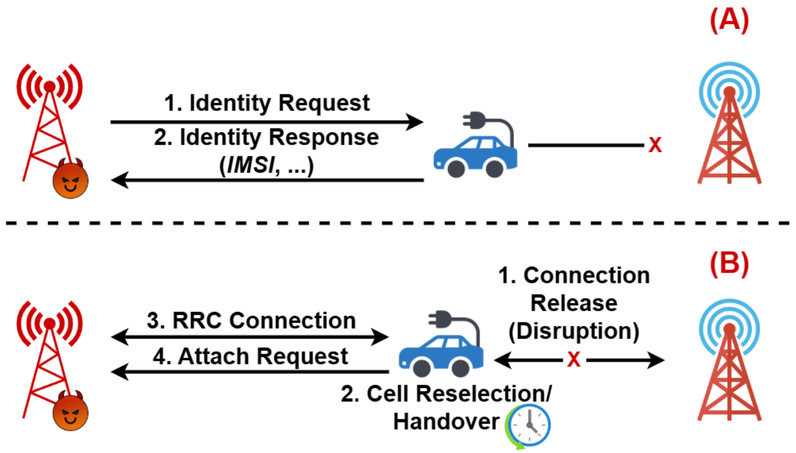
Consideration of safety & operational risks

Responsible disclosure for affected parties

Results

IMSI Catching Susceptibility

- Rogue eNodeB sent an unprotected NAS **Identity Request**
- Matching legitimate PLMNs caused disclosure of **IMSI and GUTI**
- Successful with both embedded eSIM and programmed physical SIM
- Test PLMNs such as **00101** and **99970** did not trigger disclosure
- **IMEI was not exposed**
- No user-visible indication of the identity disclosure
- Identity exposure can lead to sustained tracking and spying




```
MAC-LTE                          42 RAR (RA-RNTI=2, SFN=530 , SF=6) (RAPID=23: TA=1, UL-Grant=52236, Temp C-RNTI=73)
LTE RRC UL_CCCH                  41 RRCConnectionRequest
LTE RRC DL_CCCH                  66 RRCConnectionSetup
LTE RRC UL_DCCH/NAS-EPS         191 RRCConnectionSetupComplete, Attach request, PDN connectivity request
RLC-LTE                          41  [DL] [AM] SRB:1  [CONTROL]  ACK_SN=1
LTE RRC DL_DCCH/NAS-EPS          52 DLInformationTransfer, Identity request
LTE RRC UL_DCCH/NAS-EPS         551  [UL] [AM] SRB:1  [CONTROL]  ACK_SN=1      ||   , ULInformationTransfer, Identity response
```

Attacking PLMN	Tesla PLMN	Identity Leaked	SIM Type	Attack Result
310260	310260	IMSI/GUTI	eSIM	✓
310260	310260	IMSI/GUTI	pSIM	✓
310150	310150	IMSI/GUTI	pSIM	✓
00101	310260	None	pSIM	✗
99970	310260	None	pSIM	✗

Results

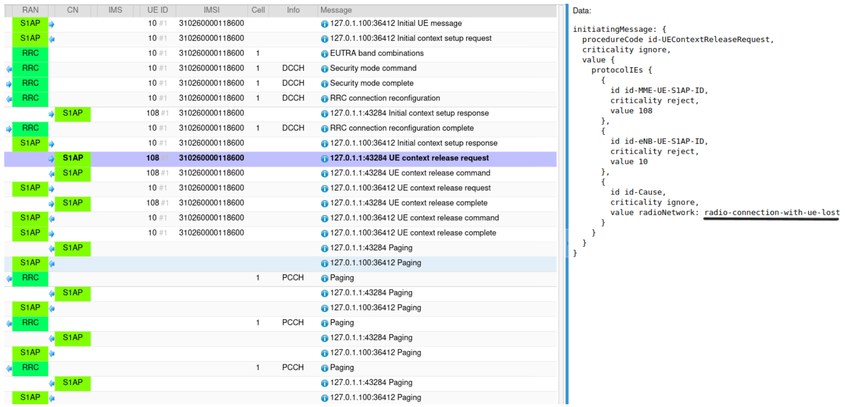
Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26

False Base Station Susceptibility

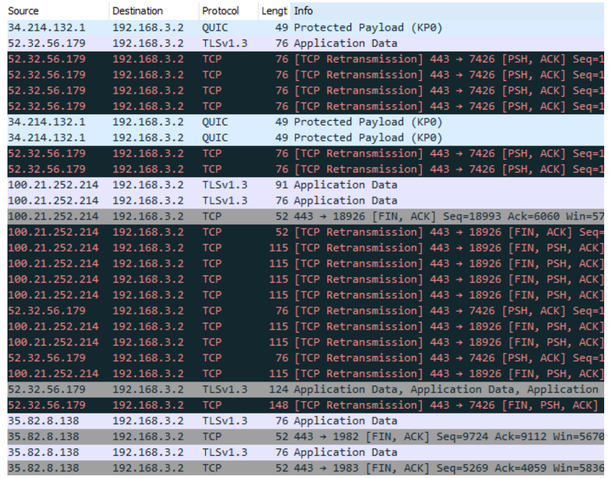
- Rogue LTE cell spoofed the vehicle's expected operator
- Signal dominance caused the TCU to select and interact with the rogue cell
- Attachment/control-plane engagement occurred in approx. **2-4.5 seconds**
- **90-100% success** under the tested signal configurations
- TCU continued camping or reattaching instead of returning to a trusted cell
- **No visual or audible warning to the driver**
- FBS attacks can lead to **DoS**, **downgrade attacks** (GSM), and **MitM**

Metric	DL cell gain (dB)			
	0	-5	-10	-15
Attach type	Partial	Partial	Partial	Partial
Time-to-attach (s)	≈ 2.0	≈ 2.0	≈ 2.5	≈ 4.5
Conn. duration (s)	≈ 4.0	≈ 4.0	≈ 4.0	≈ 4.0
Reattach / Camp	Camps	Camps	Camps	Camps
Success rate (%)	100	100	100	90



Telematics Data-Plane DoS

- Allowed LTE Control Plane while **blocking data routing**
- TCU continued sending QUIC/HTTPS traffic to Tesla backend services
- Remote-service and backend communication became **unavailable**
- **No** session termination, network reselection, or fallbacks
- Vehicle remained in the **failed state without user notification**
- Potential impact on **telemetry**, **remote commands**, **diagnostics**, and **OTA delivery**



Results

Problematic fallback behavior and Recovery

- Issues with fallbacks, loops and state transitions
- No randomized or exponential backoff was observed
- PDN failures left the TCU camped in a **partial-connectivity state**
- Routing failures produced an indefinite **data blackout**
- **No observed fallback** to: Embedded eSIM, Another PLMN, 3G, Wi-Fi
- **No** meaningful user-facing indication or recovery control

Connection Stage	Failures / Errors		
	Control	PDN	Routing
Stage 1: Attach success	✗	✓	✓
Stage 2: PDN session	–	✗	✓
Stage 3: Data connectivity	–	–	✗
Behavioral outcomes			
Fallback triggered	No	No	No
Loop trapped	Yes	Yes	No
State transition failure	Yes	Yes	Yes

Open and interactive SMS service

- Well-formed text SMS messages were delivered over LTE/IMS
- Protocol-level reception and delivery were confirmed
- TCU remained RRC-connected during the exchange
- **No message, notification, or other indication appeared to the user**
- **No user-accessible inbox, filtering, or inspection capability**
- **Interface may be externally reachable** if the vehicle MSISDN is known
- **Malformed, binary or silent SMS exposure/exploitation possible!** (*not tested due to our Ethics*)



Results

Permissive PLMN Handling under Controlled Provisioning

- With a corresponding programmed physical SIM, the TCU accepted: Commercial PLMNs, Test PLMNs (such as **00101** and **00110),** Arbitrary/non-commercial PLMNs (such as **99970)**
- Completed LTE attachment and PDN establishment
- **No security warning or restriction** was displayed

Allowlisting Bypass

- TCU implements a **two-stage connectivity policy**
- First stage permits attachment and PDN establishment
- Second stage determines whether vendor services and roaming are enabled
- **Pre-authentication** and control-plane interactions remain possible
- Spoofing an approved PLMN can bypass the effective protection
- The second allowlist behaves mainly as a **service-enablement gate**, not as a cellular security boundary

Algorithm 1 Whitelisting and roaming policy fingerprinting.

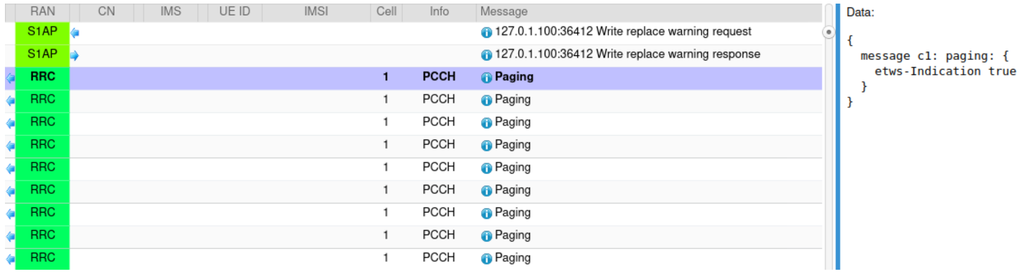
```
for all PLMN ∈ candidate_plmns do
    Configure eNodeB and EPC with PLMN parameters
    Power off Tesla vehicle network interface
    Restart LTE stack (eNodeB + EPC)
    Insert SIM programmed with same PLMN
    Power on vehicle and monitor TCU behavior
    if SIM Detected and Validated then
        Attempt for LTE Attach
        if Attach Successful then
            Attempt PDN Session Establishment
            if PDN Success then
                Verify Roaming & Cell Link State
                if Application-Layer Active then
                    Log: PLMN → Full Connectivity
                else
                    Log: PLMN → PDN, No Roaming
                end if
            else
                Log: PLMN → Attach Without PDN
            end if
        else
            Log: PLMN → Rejected at Attach
        end if
    else
        Log: PLMN → SIM Invalid
    end if
end for
```

Weak carrier policy?? Vehicle more exposed to attacks??

Results

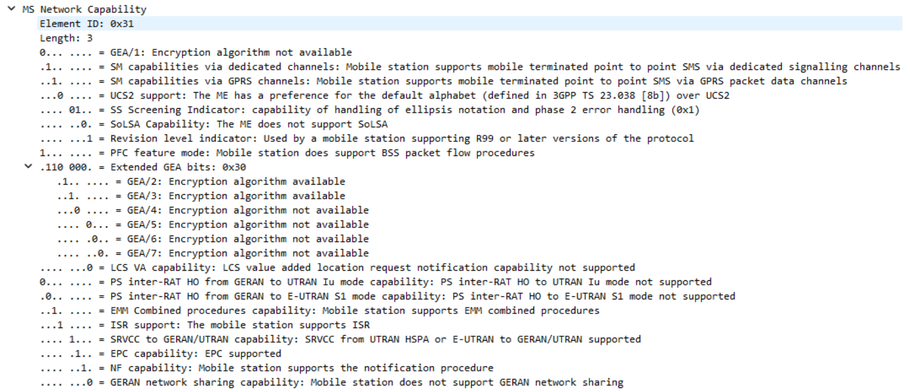
Emergency Broadcast Handling

- Transmitted normal and **spoofed ETWS/CMAS** broadcasts
- Tests performed while the vehicle was fully attached
- Transmission from the base station was confirmed
- **No visible or audible alert was produced**
- Same observation across SIM types and alert categories
- **Internal handling remains unknown**: Filtered, Silently processed, Ignored, Handled elsewhere
- **Problem**: Cellular-level emergency alerts not useful in this case



Support of GSM/2G functions and ciphers

- TCU advertised support for **GSM/2G functionality**
- Advertised legacy algorithms including **A5/3** and **GEA3**
- Also advertised support for **null ciphering**
- These capabilities increase **downgrade** and **legacy-attack exposure**
- Null integrity protection was rejected



Regulatory Concerns

Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26

Observed behaviors map to cybersecurity requirements in UN R155 and R156

Our findings map to tested threats, such as:

- Untrusted or spoofed communications
- Identity and information exposure
- Denial of service and recovery
- Legacy or insufficient cryptography
- OTA-service availability and resilience
- Recovery from connectivity disruptions
- User awareness of update-delivery failures

Identified Vulnerability	Regulatory Requirements (R155 / R156)	Mapping Justification
IMSI catching & identity exposure	R155 Annex 5 Table B1, Threat 7.1 (interception/monitoring), Mitigation M12; Vehicle-type 7.3.3, 7.3.7	Confidential identifiers must be protected; vehicle fails to mitigate interception or to provide detection/forensics.
Rogue base station & lax PLMN enforcement	R155 Annex 5 Table B1, Threat 6.1 (accepting untrusted info), 6.2 (MitM), Mitigation M10; Threat 8.1 (DoS), Mitigation M13; Vehicle-type 7.3.3–7.3.7	OEM must authenticate sources, prevent spoofing, and detect DoS; Tesla attaches to untrusted PLMNs without recovery.
Insecure fallback & attach loops	R155 Table B1 Threat 8.1 (DoS), Mitigation M13; Vehicle-type 7.3.4, 7.3.6, 7.3.7. R156 7.1.3.1–7.1.3.3, 7.2.2.1.1, 7.2.2.2, 7.2.2.4, 7.2.2.5	Persistent attach loops show lack of DoS recovery (R155) and violate R156 requirements for secure, recoverable, and user-notified OTA processes.
Legacy & weak crypto (e.g., null cipher, A5/3)	R155 Table B6 Threats 26.2/26.3, Mitigation M23; Vehicle-type 7.3.8	Legacy and null-cipher capabilities should be carefully restricted in safety-relevant communications; the tested TCU still advertises support for such capabilities.
Protocol-level SMS reception without user-visible indication	R155 Table B1 Threat 6.1, Mitigation M10; Table B4 Threat 16.2 (telematics manipulation), Mitigation M20; Vehicle-type 7.3.7	External messages should be authenticated and monitored; the reachable and user-opaque SMS interface creates an attack surface that warrants further investigation.
No user-visible alert following emergency broadcasts	R155 Table B1 Threat 6.1, Mitigation M10; Vehicle-type 7.3.6, 7.3.7	Emergency alerts from untrusted sources should be validated; spoofed ETWS/CMAS transmissions did not produce a visible or audible alert under the tested conditions, while internal handling remains unknown.
Services blocked by rogue LTE base station	R155 Table B2 Threat 13.1 (DoS vs. update rollout), Mitigation M3. R156 7.1.3.1 – 7.1.3.2, 7.2.2.1.1, 7.2.2.2, 7.2.2.4, 7.2.2.5	Disrupting access to update services is a recognized DoS threat (R155) and may affect OTA availability, recovery, and user-awareness requirements under R156.
Lack of user awareness of update failures	R156 7.2.2.2 (inform before), 7.2.2.4 (inform after)	Users should receive relevant connectivity and update-status information; Tesla provides no user-visible feedback during connectivity disruption.
Supplier-dependent stack	R155 Vehicle-type 7.2.2.5 (supplier dependencies), 7.3.2 (supplier-related risks)	R155 requires managing supplier risks; risks involving shared cellular components or integration patterns may propagate across OEMs, not just Tesla.

What about other standards?

ISO

Countermeasures

Upgrade to 5G as default 

Use stricter carrier policy 

Remove unnecessary services (e.g, SMS) 

Remove weak configurations completely (e.g, GSM ciphers) 

Fix the fallback logic with health monitoring 

Impose stricter control on physical SIM cards, favor eSIMs 

Improve the interface with the user (e.g., notifications, awareness, control) 

Ensure compliance with the standards and policies 

Takeaways

Northeastern University
Khoury College of Computer and Information Sciences

WOOT '26



Production vehicles are testable



Classical cellular risks remain relevant



Implementation flaws & misconfigurations



Standards conformity & adherence



Safety requirements need further investigation



Limited driver visibility / little attention from diagnostics

Artifact

ARTIFACT EVALUATED
USENIX
AVAILABLE

Thank You !