International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

СЛАБОСТИ В ЗАЩИТАТА НА КОМУНИКАЦИОННИТЕ ЛИНИИ (CAN, RF АНТЕНИ И ДР.) И ДОСТЪП ДО УЯЗВИМИ ЕЛЕМЕНТИ НА ИМОБИЛАЙЗЕРНИТЕ СИСТЕМИ НА ПРЕВОЗНИТЕ СРЕДСТВА

инж. Страхил Събев

ТУ – Габрово, Габрово, България
strahilsubev@gmail.com

VULNERABILITIES OF COMMUNICATION LINKS AND ACCESSIBLE COMPONENTS IN VEHICLE IMMOBILIZER SYSTEMS

eng. Strahil Sabev

TU Gabrovo, Gabrovo, Bulgaria
strahilsubev@gmail.com

Abstract

This paper presents an engineering analysis of vehicle immobilizer security across radio interfaces, internal communication networks and accessible electronic modules. Block diagrams identify the authentication path and trust boundaries. Attacks and defenses are classified by affected interface and security function. Equivalent electrical circuits illustrate a Controller Area Network (CAN) segment and a resonant low-frequency antenna. Analytical relationships connect bus termination, antenna tuning and distance estimation to measurable diagnostic quantities. The analysis distinguishes electrical integrity from message authenticity and key authentication from proof of proximity. A verification procedure relates threats to controls, observable parameters and acceptance criteria. The study synthesizes published research and component documentation; the numerical examples are calculations rather than experimental measurements.

Keywords: immobilizer; CAN; passive keyless entry; RF; UWB; SecOC; vehicle cybersecurity.

ВЪВЕДЕНИЕ

Имобилайзерът е многокомпонентна система за предотвратяване неоторизирано движение на автомобила. Удостоверяването на ключа, обменът между модулите и крайното разрешение са отделни етапи. Слабости във всеки от тях може да наруши защитата, без непременно да бъде разкрит криптографският ключ.

Обект на анализа са мрежата от контролери (Controller Area Network, CAN), радиочестотните интерфейси (Radio Frequency, RF) и достъпните електронни модули. Разглеждат се целостта на съобщенията, доказването на близост и контролът върху сервизните операции [1–4].

Целта е да се покажат архитектурата, класовете атаки и методите за защита чрез възможни инженерни решения. Представени са блокови и принципни електрически схеми, класификации и критерии за изпитване.

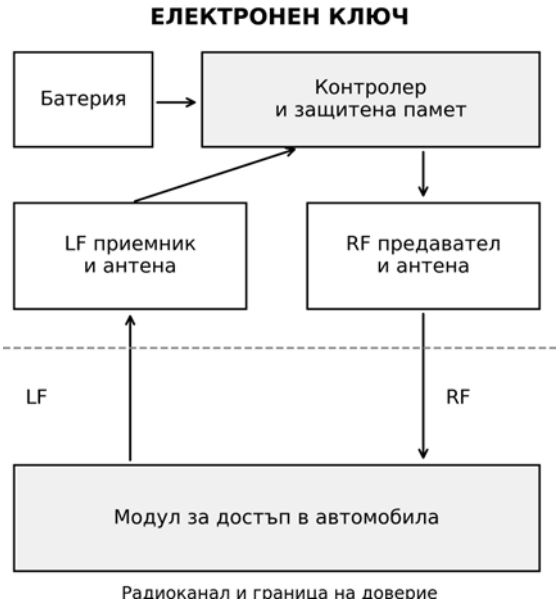
Анализът използва научни подходи, методи от практиката и техническа документация. Изложените слабости не се приемат като еднаква уязвимост на всички автомобили поради многото различни подходи на производителите.

Print ISSN: 1313-230X, Online ISSN: 3033-1404

ИЗЛОЖЕНИЕ

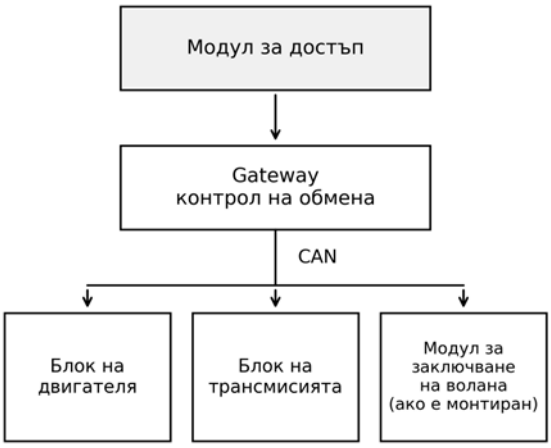
1. АРХИТЕКТУРА

Фиг. 1 показва типична реализация на пасивен достъп и стартиране (Passive Entry Passive Start, PEPS), наричана и Passive Keyless Entry and Start (PKES). Нискочестотният канал (Low Frequency, LF) приема заявка от автомобила, а RF каналът връща отговора на ключа [3].



Фиг. 1. *Блокова схема на електронен ключ с LF приемане и RF предаване*

Контролерът обработва заявката и връща обратно отговор със защитени идентификационни данни. Батерията захранва активните функции. Отделният пасивен транспондер за резервно стартиране, когато е наличен, не е показан в обобщената схема и работи, чрез друга малка антена.



Фиг. 2*. Обмен между модули при разрешаване на стартирането; обобщена архитектура*

2. КЛАСИФИКАЦИЯ НА АТАКИТЕ

Класификацията на фиг. 3 групира методите по засегнат интерфейс. Физическият достъп е предварително условие за част от сценариите, а не отделен начин за атака. Под-методите имат различни последствия [1–4].



Фиг. 3*. Класове атаки и основни подметоди*

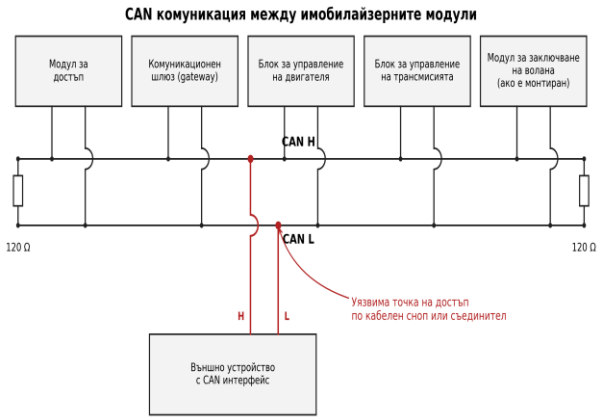
Препредаването копира и модифицира текущ обмен между автомобила и валиден ключ. Повторението използва записан по-рано обмен. Подмяната на съобщение променя данни или имитира източник, а заглушаването и претоварването засягат наличността на комуникацията.

При модулите се разграничават замяна на устройство, достъп до незащитена памет и използване на диагностична функция с недостатъчни проверки. Всеки сценарий се оценява чрез необходимия достъп, засегнатите модул, данни и възможното последствие.

Комуникационният шлюз (gateway) на фиг. 2 свързва мрежови сегменти. Той трябва да допуска само разрешения обмен. Реалното разпределение на функциите и наличието на отделни модули зависят от конкретния автомобил.

3. СЛАБОСТИ НА ВЪТРЕШНАТА КОМУНИКАЦИЯ

Класическият CAN осигурява връзка и контрол на грешки, но рамката по подразбиране не удостоверява изпращача на командата криптографски. Ако недоверено устройство получи достъп до съответния канал, може да наблюдава сигналите за сигурност и при определени условия да изпраща съобщения със същите идентификатори като легитимен блок. Това е свойство на този тип мрежа, а не универсална уязвимост на всеки имобилайзер.



Фиг. 4. *CAN комуникация между модулите на имобилайзера и свързване на външното устройство от фиг. 5 към шината.*



Фиг. 5*. Достъп със сонди до вътрешната CAN шина на автомобил с цел извличане на данни от имобилайзера*

Особено важен е мостът между достъпна периферия и модули, участващи в разрешаването на старта. Физически изложен кабелен сноп или свързан външен контролер може да увеличи риска, когато шлюзът изпраща команди, свързани със сигурността, и получаващият модул приема неудостоверено съобщение. Защитата на OBD порта не покрива непременно всички други точки на включване.

Повторението на предишни съобщения и подмяната на състояние са отделни уязвимости на системата. Логиката за опресняване и криптографският код за автентичност обвързват съобщението с актуална сесия, но изискват управление на ключовете и синхронизация. Защитената бордова комуникация (Secure Onboard Communication, SecOC) в архитектурата AUTomotive Open System ARchitecture (AUTOSAR) дефинира механизъм за удостоверяване и защитава обхванатите съобщения от подмяна и повторение при правилно управление на ключовете [5].

Кодът за автентичност на съобщението (Message Authentication Code, MAC) се изчислява със секретен ключ. Приемането изисква едновременно валиден MAC и допустим времеви прозорец [5].

Системата за откриване на прониква-

ния (Intrusion Detection System, IDS) допълва удостоверяването чрез анализ на периодичност, съдържание и контекст. Тя не замества криптографската проверка. Прекъсване или претоварване на шината остава възможно и при защитени съобщения [1, 2].

4. RF КАНАЛИ И ПАСИВЕН ДОСТЪП

При релейна атака валидният ключ участва в текущия обмен, но се намира извън очакваната зона, защита е измерване на дистанцията на ключа. Защото успешната криптографска проверка не е равнозначна на доказана реална близост на физическият ключ [3].



Фиг. 6. *Илюстрация на препредаване на сигнала между автомобила и валидния ключ*

Bluetooth с ниска консумация на енергия (Bluetooth Low Energy, BLE) може да служи за откриване и обмен на данни. Свръхширококолентовата радиотехнология (Ultra-Wideband, UWB) позволява оценка на разстоянието чрез време на полет (Time of Flight, ToF). Комбинацията BLE/UWB се използва и при дигитални ключове в съвместими мобилни устройства [10].

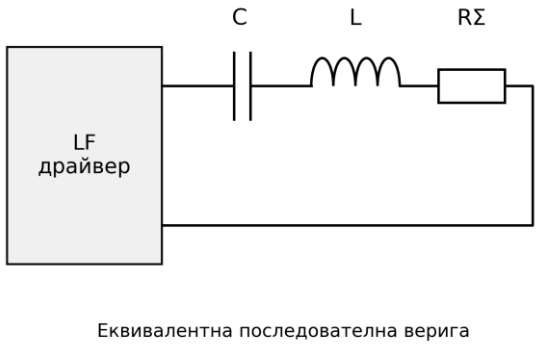
$$d \approx \frac{c \cdot (t_{RT} - t_{отг})}{2} \qquad (1)$$

Тук d е разстоянието, $c \approx 3 \times 10^8$ m/s, t_{RT} е измереното време за двупосочния обмен, а $t_{отг}$ е закъснението на отговора.

При грешка 1 ns в коригираното двупосочно време означава приблизително 0,15 m грешка в d.

Измерването трябва да отчита закъсненията в електрониката и условията на разпространение. Прагът за отключване и разграничаването между салона и външната зона се проверяват отделно за конкретната система.

4.1. Резонансна LF антена



Фиг. 7. *Еквивалентна схема на LF антена с последователен резонанс [9]*

L е индуктивността на антената, C е настройващият капацитет, а R_Σ обобщава загубите в намотката и веригата. Схемата показва принципа, без да задава свързване към конкретни изводи на автомобилен модул.

$$f_0 = \frac{1}{2\pi\sqrt{LC}} \qquad (2)$$

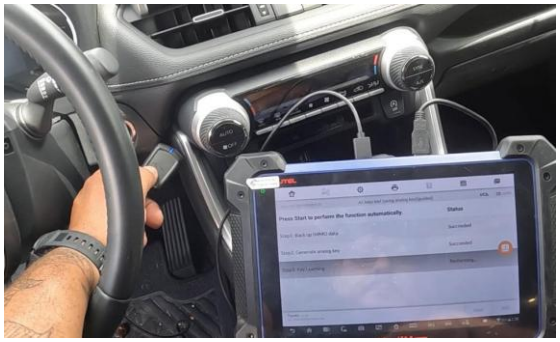
За примерни $L = 1\,\text{mH}$ и $f_0 = 125\,\text{kHz}$ се получава $C \approx 1{,}62\,\text{nF}$. Това е изчислителен пример, а не универсален номинал. Реалните характеристики отчитат толерансите, паразитните параметри, тока и ограниченията на драйвера [9].

Прекъсване, късо съединение или изменение на L и C променя тока и наст-

ройката. Контролът на тези величини може да установи електрическа аномалия, но сам по себе си не различава повреда от умишлена намеса. Анализът на LF сигнала е изследван и като допълнителен метод за откриване на препредаване [6].

5. ДОСТЪП ДО МОДУЛИ И ДИАГНОСТИКА

Портът за бордова диагностика (On-Board Diagnostics, OBD) е само една възможна входна точка. Достъпът до свързващ елемент, кабелен сноп или демонтиран блок създава различни условия за намеса. Оценката включва паметта, сервизните функции и връзките към останалите модули.



***Фиг. 8**. Работ с емулатор на електронен ключ и диагностично оборудване*

Обучението на ключ и адаптацията на контролер трябва да изискват удостоверен достъп, конкретни права и регистрация на операцията. Постоянен общ секрет за множество устройства увеличава значително риска от компрометиране. Защитеното съхранение и уникалните ключове ограничават този риск.

Проверката при подмяна на модул обхваща неговата идентичност, разрешената конфигурация и състоянието на софтуера. Подписаните от производителя дигитално обновявания и защитеното стартиране намаляват вероятността от изпълнение на неподходящ код. Необходимо е да остане контролиран път за законен ремонт.

След сервизна намеса (фиг. 8) се проверяват броят на разрешените ключове, успешното разпознаване на валидния ключ и отказът при невалидна идентификация. Резултатите се свързват с конкретната конфигурация на модулите.

6. КЛАСИФИКАЦИЯ НА ЗАЩИТИТЕ

Фиг. 9 разделя защитите според тяхната функция. Една мярка може да участва в повече от един клас. Целта е пропуск в един слой да бъде ограничен от останалите.



***Фиг. 9**. Графична класификация на защитите*

Предотвратяването включва удостоверяване на ключа и съобщенията, ограничаване на диагностичните права и разделяне на мрежовите сегменти. Защитата на секретите се прилага както в ключа, така и в автомобилния модул.

Откриването обединява IDS, контрол на електрическите линии и журнал на значимите операции. Сигналът за аномалия се съпоставя с режима на автомобила, наличието на валиден ключ и разрешена сервизна сесия.

Ограничаването включва отхвърляне

на невалидни команди и изолация на засегнатия сегмент, когато това е безопасно. Възстановяването предвижда отмяна на компрометирани права и контролирана адаптация. Реакцията не трябва да води до опасно спиране на двигателя в движение.

ЗАКЛЮЧЕНИЕ

Надеждната защита изисква отделна проверка на електрическата изправност, автентичността на съобщенията, близостта на ключа и правата за ремонт и замяна. Предложените схеми и критерии дават основа за изпитване на стенд при конкретна архитектура. Ефективността трябва да се потвърди с измервания, включително при нормална експлоатация и откази.

ЛИТЕРАТУРА

[1] Sharmin, S., Mansor, H., Abdul Kadir, A. F., Aziz, N. A. Benchmarking Frameworks and Comparative Studies of Controller Area Network (CAN) Intrusion Detection Systems: A Review. 2024. arXiv:2402.06904. https://arxiv.org/abs/2402.06904

[2] Liu, Y. et al. Vehicular Intrusion Detection System for Controller Area Network: A Comprehensive Survey and Evaluation. IEEE Transactions on Intelligent Transportation Systems, 2025. doi:10.1109/TITS.2025.3567940.

[3] Francillon, A., Danev, B., Capkun, S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium, 2011. https://www.ndss-symposium.org/ndss2011/relay-attacks-on-passive-keyless-entry-and-start-systems-in-modern-cars/

[4] Leu, P. et al. Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging. USENIX Security Symposium, 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/leu

[5] AUTOSAR. Specification of Secure Onboard Communication. Classic Platform, R24-11, 2024. AUTOSAR_CP_SWS_SecureOnboardCommunication.pdf. https://www.autosar.org/standards/classic-platform/

[6] Joo, K., Jo, H. J., Choi, W. Securing Passive Keyless Entry and Start System in Modern Vehicles Based on LF-Band Signal Analysis. IEEE Internet of Things Journal, 11(24), 40176–40190, 2024. doi:10.1109/JIOT.2024.3453920.

[7] United Nations Economic Commission for Europe. UN Regulation No. 155: Cyber Security and Cyber Security Management System. 2021. https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[8] Texas Instruments. TCAN1042-Q1 Automotive Fault Protected CAN Transceiver with CAN FD. Datasheet SLLSES9D, Rev. D, 2021, Section 10.2. https://www.ti.com/lit/gpn/TCAN1042-Q1

[9] Microchip Technology. ATA5279/ATA5279C: Antenna Driver for Multiple Antennas. Datasheet, document 9125. https://www.microchip.com/en-us/product/ata5279c

[10] Car Connectivity Consortium. Car Connectivity Consortium Publishes Digital Key Release 3.0. 13 July 2021. https://carconnectivity.org/car-connectivity-consortium-publishes-digital-key-release-3-0-businesswire/