Авдалян А.А. Как можно взломать автомобильный брелок через SDR (SOFTWARE DEFINED RADIO)? // Международный журнал информационных технологий и энергоэффективности.– 2025. –Т. 10 № 4(54) с. 70–73

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.5

КАК МОЖНО ВЗЛОМАТЬ АВТОМОБИЛЬНЫЙ БРЕЛОК ЧЕРЕЗ SDR (SOFTWARE DEFINED RADIO)?

Авдалян А.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: sharmanka228@gmail.com

Современные автомобильные брелоки используют радиосигналы для разблокировки и запуска транспортных средств, но недостаточная защита этих сигналов делает возможным их перехват и повторное воспроизведение с помощью SDR (Software Defined Radio). В статье рассматриваются основные уязвимости автомобильных брелоков, методы их взлома с использованием SDR, такие как атаки повторного воспроизведения (replay attack) и атаки на слабые алгоритмы шифрования, а также предлагаются меры защиты от подобных угроз.

Ключевые слова: Автомобильный брелок, SDR, радиоперехват, повторная атака, уязвимости, кибербезопасность, программно-определяемое радио.

HOW TO HACK A CAR KEY FOB USING SDR (SOFTWARE DEFINED RADIO)?

Avdalyan A.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: sharmanka228@gmail.com

Modern car key fobs use radio signals to unlock and start vehicles, but weak security measures make it possible to intercept and replay these signals using SDR (Software Defined Radio). This article explores the main vulnerabilities of car key fobs, hacking methods using SDR, such as replay attacks and exploits on weak encryption algorithms, and suggests protection measures against such threats.

Keywords: Car key fob, SDR, radio interception, replay attack, vulnerabilities, cybersecurity, software-defined radio.

Введение

Развитие беспроводных технологий значительно повысило удобство использования автомобилей, позволяя владельцам открывать двери и запускать двигатель с помощью радиоуправляемых брелоков. Однако эта же технология открыла новые уязвимости, которыми могут воспользоваться злоумышленники. Программно-определяемое радио (SDR) стало мощным инструментом в руках специалистов по кибербезопасности, хакеров и исследователей, позволяя перехватывать и анализировать радиосигналы автомобильных систем. В отличие от традиционных приёмников, SDR позволяет программно изменять параметры работы, что делает его универсальным инструментом для изучения и потенциального взлома радиочастотных систем.

Уязвимости в автомобильных брелоках могут привести к угону транспортных средств или несанкционированному доступу к их системам. Некоторые модели автомобилей до сих пор используют устаревшие алгоритмы кодирования сигнала, которые легко взломать при наличии соответствующего оборудования и знаний. Атаки с использованием SDR могут включать в себя перехват радиосигнала, его запись и повторное воспроизведение, что позволяет злоумышленникам разблокировать автомобиль без наличия оригинального брелока. В этой статье мы рассмотрим основные методы взлома автомобильных брелоков через SDR и способы защиты от подобных атак.

Как можно взломать автомобильный брелок через SDR?

Одним из наиболее распространённых методов взлома автомобильных брелоков с помощью SDR является атака повторного воспроизведения (replay attack). Этот метод особенно эффективен против устаревших систем, использующих фиксированные или слабо защищённые сигналы. Атака начинается с того, что злоумышленник использует SDR-приёмник для перехвата радиосигнала, передаваемого брелоком при нажатии кнопки разблокировки. Затем этот сигнал записывается и воспроизводится в нужный момент, что позволяет злоумышленнику открыть автомобиль без оригинального брелока[1].

Для осуществления подобной атаки могут использоваться недорогие SDR-устройства, такие как RTL-SDR, HackRF One или BladeRF. Эти устройства позволяют улавливать радиочастоты, на которых работают автомобильные брелоки (обычно в диапазоне 300–500 МГц). С помощью специализированного ПО, например GNU Radio или Universal Radio Hacker, злоумышленник может анализировать захваченные сигналы, фильтровать их и в дальнейшем использовать для атаки[2].

Другой метод атаки — анализ и взлом слабых алгоритмов кодирования сигнала. Некоторые автомобили используют устаревшие механизмы защиты, такие как фиксированные коды (fixed code), которые остаются неизменными при каждом нажатии кнопки брелока. Если злоумышленник перехватит такой сигнал один раз, он может воспроизвести его сколько угодно раз, что делает защиту автомобиля неэффективной. Современные системы применяют кодировку с "плавающим кодом" (rolling code), при которой каждый новый сигнал уникален и не может быть повторно использован. Однако и такие системы имеют уязвимости: злоумышленник может использовать атаку "rolljam", в ходе которой перехватываются несколько последовательных сигналов, что позволяет в дальнейшем скомпрометировать систему[3].

Для выполнения атаки rolljam злоумышленник использует два приёмника SDR: один записывает сигнал от брелока, а второй одновременно глушит передачу сигнала к автомобилю. Таким образом, владелец вынужден нажимать кнопку несколько раз, и атакующий получает несколько уникальных кодов. Один из этих кодов используется для разблокировки автомобиля, а второй сохраняется для последующего использования. Данный метод делает возможным угон даже автомобилей, использующих более современные методы защиты[4].

Помимо атак replay attack и rolljam, SDR также позволяет проводить анализ радиосигнала с целью поиска других уязвимостей. Например, некоторые брелоки и системы бесключевого доступа (keyless entry) передают сигналы в некодированном виде, что позволяет их относительно легко клонировать. В некоторых случаях злоумышленники могут даже

использовать ретрансляционные атаки (relay attack), при которых сигнал от ключа перехватывается и передаётся на большее расстояние, позволяя разблокировать и завести автомобиль, даже если оригинальный ключ находится далеко от машины[5].

В связи с развитием SDR-технологий и их доступностью защита автомобильных систем становится важнейшей задачей для производителей транспортных средств. Компании, занимающиеся автомобильной безопасностью, внедряют усовершенствованные механизмы шифрования и защиты сигналов, однако старые модели автомобилей всё ещё остаются уязвимыми. Владельцам транспортных средств следует учитывать возможные угрозы и предпринимать дополнительные меры защиты.

Заключение

Использование SDR для взлома автомобильных брелоков подчёркивает уязвимость современных транспортных средств перед радиочастотными атаками. Злоумышленники могут использовать методы replay attack, rolljam и relay attack для получения несанкционированного доступа к автомобилю. Эти атаки становятся всё более доступными из-за распространённости SDR-устройств и программного обеспечения для анализа радиосигналов.

Чтобы минимизировать риск взлома, производители автомобилей внедряют новые технологии защиты, такие как улучшенные алгоритмы шифрования и системы обнаружения аномальной активности. Однако владельцам автомобилей также следует предпринимать меры предосторожности: хранить брелоки в экранированных чехлах, отключать бесключевой доступ, если он не используется, и регулярно обновлять программное обеспечение бортовых систем.

Развитие SDR-технологий открывает не только новые возможности в радиосвязи, но и создаёт серьёзные вызовы для автомобильной безопасности. Важно понимать потенциальные угрозы и активно внедрять методы защиты, чтобы предотвратить угон автомобилей с использованием уязвимостей в радиосистемах.

Список литературы

1. Богомаз М. Э., Михайлова Л. А., Поляничева А. В. ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ IP-ТЕЛЕФОНИИ //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 170-172.
2. Волкогонов В. Н. и др. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.
3. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657.
4. Леснова Е. М., Пестов И. Е. Разработка метода обнаружения и коррекции ошибок для распределенной информационной сети на основе больших данных //Региональная информатика и информационная безопасность. – 2018. – С. 236-240.
5. Кушнир Д. В. Исследование и разработка методов распределения конфиденциальных данных по квантовым каналам : дис. – Санкт-Петербург. гос. ун-т телекоммуникаций им. МА Бонч-Бруевича, 1996.

References

1. Bogomaz M. E., Mikhailova L. A., Polyanicheva A.V. IP TELEPHONY SECURITY TOOLS //Actual problems of infotelec communications in science and education (APINO 2022). – 2022. – pp. 170-172.
2. Volkogonov V. N. et al. The use of physically non-cloned functions to perform authentication in the Internet of Things environment //Actual problems of infotelec communications in science and education. - 2021. – pp. 409-414.
3. Sinelshchikov V. S., Tsvetkov A. Yu. Personal data protection at the enterprise //Actual problems of infotelec communications in science and education (APINO 2021). – 2021. – pp. 653-657.
4. Lesnova E. M., Pestov I. E. Development of an error detection and correction method for a distributed information network based on big data //Regional Informatics and information security. 2018. pp. 236-240.
5. Kushnir D. V. Research and development of methods for distributing confidential data through quantum channels : St. Petersburg State University of Telecommunications named after MA Bonch-Bruevich, 1996.