ДК 004.056.5:629.3 **doi:**

СИСТЕМА PKES АВТОМОБІЛЯ ТА СПОСОБИ ЇЇ ЗАХИСТУ ВІД ЗЛОВМИСНОГО ВТРУЧАННЯ

Левтеров А.І., Іванов С.М.
Харківський національний автомобільно-дорожній університет

Анотація: Розглянуто систему безключового доступу до автомобіля. Запропоновано нову методику захисту від зловмисників цієї системи введенням до смарт-ключа та іммобілайзера додаткових елементів та розглянуто роботу оновленої системи.
Ключові слова: смарт-ключ, транспондер, іммобілайзер, регістр пам’яті зі зсувом, зондуюча антена, ретранслятор, емулятор, криптопароль.

Вступ

Сучасні автомобілі є найкращим прикладом кіберфізичної системи через інтеграцію обчислювальних компонентів і фізичних систем. Інакше кажучи, автомобілі нашого століття, це комп'ютери, які керують технологічною обвіскою - двигуном і гальмами, фарами і поворотниками, двірниками і кондиціонером, та й рештою теж [1]. Їх сміливо можна порівняти з сучасними комп'ютерами, що мають складну електронну начинку. Але «розумні», машини перетворюються на досить ласу мішень для хакерів [2]. За даними всесвітньої організації *ISO/SAE 21434:2021* кіберзлочинність завдає шкоди світовій економіці на суму 500 млрд. євро щорічно [3].

Аналіз публікацій

Відмички, монтировка та розбите скло – це вже в минулому. Сьогодні для зламу автомобілів все частіше використовуються ноутбуки та спеціальне комп'ютерне обладнання. Наприклад, у Лондоні ще в 2015 році зловмисники, зробивши дублікат радіобрелка для розблокування іммобілайзера, викрали понад 6000 автомобілів. Система безключового доступу до автомобіля (СПДА) стала дуже популярною функцією у багатьох нових автомобілях. Вона дозволяє водієві без використання ключа відчиняти двері і заводити машину завдяки маленькому електронному брелку, що лежить у кишені одягу або в сумці водія, який обмінюється даними по радіохвилях з автомобілем, що дозволяє відкривати двері і запускати двигун і так далі без ключа [2].

Як правило, автовиробники комплектують свої нові автомобілі радіо-брелками (смарт-ключами) (за галузевою термінологією такі системи називаються PKES – Passive Keyless Entry and Start – «пасивний безключовий доступ і запуск двигуна» [4]), які, працюючи по радіоканалу, повідомляють сигналізації машини, що до нею підходить її автовласник. Якщо код у них збігається, сигналізація відключається і у автомобіля автоматично відкриваються двері.

Це посилання передається в ефір на чистоті 125 кГц і, якщо ключ-брелок знаходиться поруч і розуміє мову запиту, він відразу відповідає машині, використовуючи вже свою робочу частоту (433 або 868 МГц). Причому відповідає хитрою цифровою комбінацією, що згенерована за індивідуальним алгоритмом шифрування.

Щоб виключити електронні підтасовки, відповідь від електронного ключа має надійти в режимі реального часу (рахунок затримок ведеться на наносекунди), тому будь-які спроби відкрити машину приречені на провал. Але навіть такі хитромудрі дії не завжди рятують від угону. [3]. Кількість викрадень машин з безконтактною системою доступу зростає у геометричній прогресії [2] і займає третє місце по числу кібератак [4].

Так, згідно з проведеним дослідженням Швейцарським технологічним інститутом вдалося встановити, що сучасні PKES, що дозволяють водієві автоматично відчиняти

двері в машині і запускати двигун без ключа, дуже вразливі для зламу безпосередньо через радіоканал [5].

Щоб протестувати електронний захист автомобілів, фахівці інституту відібрали десять ключів-брелків (від 10 автомобілів) від 8 марок автомобілів. Тестування відбувалося без участі представників автомобільних компаній. Завдяки цьому експерименту Швейцарська команда інженерів продемонструвала конкретний метод, який дозволив їм зламати (відкрити) усі без винятку вибрані автомобілі, які брали участь у цьому випробуванні.

Саме ці тести показали, що смарт-ключи дистанційного відчинення дверей (PKES) при наближенні власника до автомобіля, досить-таки нескладно зламати за допомогою спеціального способу та відповідного обладнання.

Щоб відкрити автомобіль за допомогою сигналу з нерідного ключа автомобільному злодієві знадобиться помічник і спеціальний прилад – ретранслятор (рис.2) [6,7].

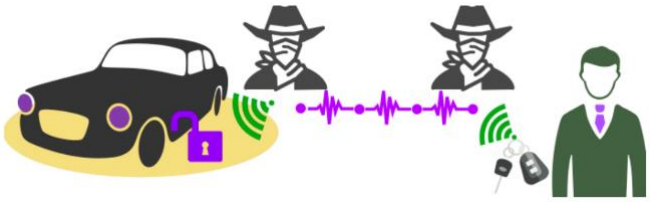

Рис. 2. «Операція» відкриття автомобіля

Помічник під час «операції» знаходиться поряд із власником автомобіля (смарт-ключем). Він встановлює цифровий зв'язок із пристроєм. Його учасник біля автомобіля натискає кнопку відкриття дверей. Сигнал обробляється в ретрансляторі та відправляється помічнику, який, підтримуючи зв'язок із ключем, пересилає сигнал назад. Ця схема спрацьовує практично на будь-яких авто. Схематично це виглядає так (рис. 3, рис. 4) [8].

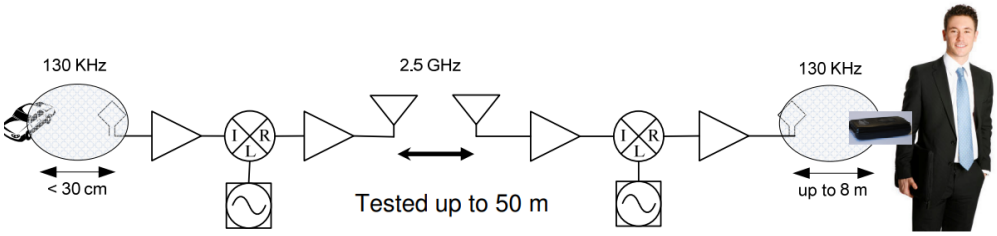

Рис.3. Схема безключового відкриття автомобіля

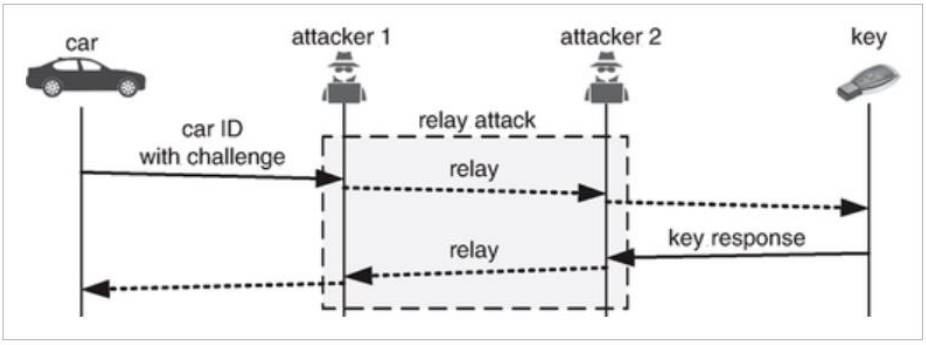

Рис. 4. Схема ретрансляції сигналу між двома зловмисниками

Пристрій коштує пристойних грошей, але успішне викрадення автомобіля все окупає. На рис.5. показано обладнання, яке було представлене на міжнародній виставці, що проходила у Польщі [9].

Виставка була присвячена технологіям відкриття автомобілів без оригінального ключа. На виставці були присутні автомайстри із багатьох Європейських країн.

Рис.5. Комплект обладнання для відкриття автомобілів без оригінального ключа-брелка

Розглянемо проведення «операції» відкриття автомобіля докладніше на конкретному прикладі.

Після включення охоронної сигналізації блоки встановлюють між собою високошвидкісний канал передачі даних, що дозволяє ретранслювати ключові запити автомобіля і віддалено приймати відповіді мітки.

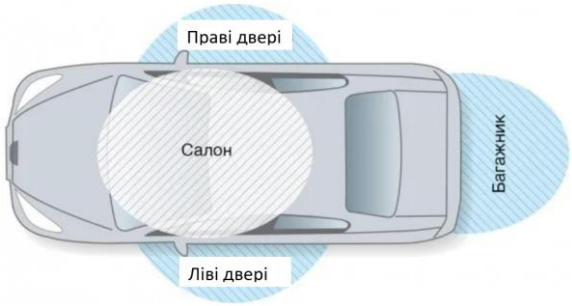

Рис.6. Зондуючі антени, встановлені в автомобілі

Зондуючі антени на 125 кГц встановлені по периметру кузова так, щоб їх діаграми не перекривалися (рис.6) [10]. Завдяки цьому машина завжди знає, звідки відповідає ключ, і дозволяє виконання лише "географічно прив'язаних" команд. Наприклад, двигун запуститься в тому випадку, якщо в радіообміні з ключем буде задіяна антена в спинці сидіння водія, а багажник відкриється лише при успішному опитуванні ключа із заднього сектора.

Для викрадення злочинці використовують спеціальні ретранслятори, які, перехоплюючи сигнал з безконтактних ключів, посилюють спійманий сигнал, а потім передають його на радіоприймач, який у свою чергу ретранслює сигнал на автомобіль (рис.3, рис.4) [8]. Зрештою охоронна система приймає рідний сигнал безконтактного ключа, який може в цей момент перебувати далеко від автомобіля. Наприклад, за допомогою подібних ретрансляторів зловмисники можуть передати сигнал з ключа-брелка, коли водій перебуває на роботі, в кафе, ресторані, магазині, кінотеатрі і т.д. Можна навіть змусити електронний пароль відгукнутися з закритого приміщення.

Ліворуч «емулятор», а праворуч – «зчитувач» (Рис.3), які можуть бути представлені у вигляді нехитрих коробочок. Усередині цих коробочок заховані приймачі та передавачі

на три діапазони (125 кГц, 433 МГц та 900 МГц), смугові фільтри, підсилювачі, процесори, літій-полімерні батареї великої ємності та рамкова антена. Після включення живлення блоки встановлюють між собою високошвидкісний канал передачі даних, який дозволяє ретранслювати ключові запити автомобіля і віддалено приймати відповіді мітки. На рис.7 наведено приклади реалізації протоколів обміну між автомобілем та ключем [11].

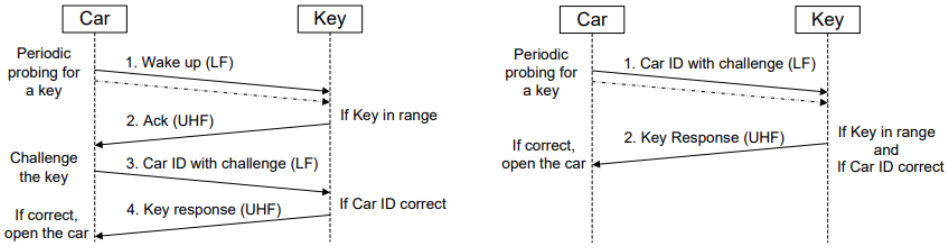

Рисунок 7. Приклади реалізації протоколу системи пасивного доступу без ключа:

a) У типовій реалізації автомобіль періодично прощупує канал на наявність ключа короткими маячками. Якщо ключ всередині діапазону, протокол запиту-відповіді між автомобілем і ключем надає або забороняє доступ (є енергоефективним, оскільки виявлення ключів залежить від дуже коротких маяків);

b) В другій реалізації автомобіль періодично зондує канал безпосередньо за допомогою потужних маяків, які містять автомобіль ідентифікатор. Якщо ключ знаходиться в зоні дії, він безпосередньо відповідає на виклик.

Творці кримінального радіоподовжувача добре знаються на питаннях електромагнітної сумісності. Під час роботи «Довгої руки/ключа» (рис.8) можна говорити по мобільному телефону або, навпаки, включати генератори перешкод стільникового зв'язку для блокування GSM-трафіку систем моніторингу [12].

Це посилання передається в ефір на «транспондерній» частоті 125 кГц і, якщо смарт-ключ знаходиться поруч і розуміє мову запиту, він відразу відповідає машині, використовуючи вже свою робочу частоту (у нас і в Європі це 433 МГц або 868 МГц), наприклад, код відповіді X123.Y456.Z789.

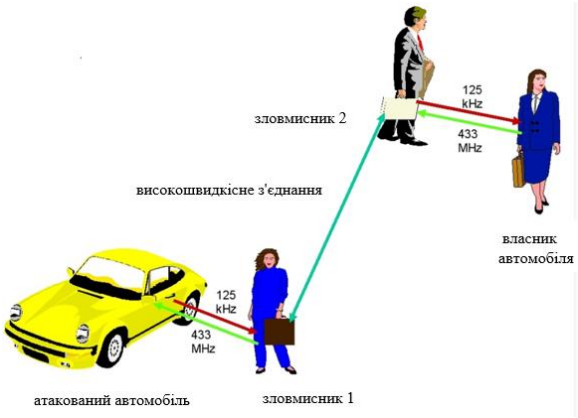

Рис. 8. Схема роботи Relay Station Attack (Технологія довгої руки/ключа)

При цьому не має значення, де знаходиться ключ - чи знаходиться він усередині будівлі, наприклад: будинку, офісу, або в кишені, сумці або файлі власника, вловити сигнал через сканер/підсилювач можна навіть з відстані 8 метрів від ключа. Посилення сигналу настільки сильне, що його можна передати на другий приймач/передавач поруч із автомобілем на відстані до 800 метрів! Автомобіль "думає", що власник відкриває

двері автомобіля заводським смарт-ключом. Перед запуском двигуна система доступу повинна ще раз запросити ключ (через антену в спинці сидіння водія), тому «емулятор» повинен бути поруч. Злодії діють неймовірно швидко. Крадіжка займає в середньому 6 секунд!

Мета і постановка завдання

Метою даної статті є пропозиція методу захисту автомобіля від несанкціонованого безключового доступу.

Відповідно до поставленої мети слід розробити методику і пристрій захисту від зловмисників для цієї системи введенням до смарт-ключа та іммобілайзера додаткових елементів.

Рішення проблеми

Що робити, щоб зв'язати викрадачам їхні довгі руки? Для цього пропонується кілька способів захисту [13].

Найрадикальнішим, мабуть, є відключення системи PKES, витягнувши з смарт-ключа батарейку!

Другий спосіб, після закриття автомобіля ховати брелок від машини в клітину Фарадея: чохол чи футляр з металевим (фольгованим) екраном. Такий притулок для «золотого ключика» можна зробити і самому – хоч би з цигаркової пачки чи рулону побутової фольги. Однак ці обидва способи дуже незручні при їх експлуатації.

Наступні три способи відносяться до системи кодування інформації та паролів. Сигнал від смарт-ключа є своєрідним паролем, що зчитується блоком керування. Ці паролі бувають трьох типів [11]:

- пароль ID (ідентифікаційний);
- змінний пароль;
- шифрований криптопароль.

Ідентифікаційний пароль записаний у чіпі ключа та в блоці іммобілайзера. Він не змінюється і завжди однаковий. Зловмисники можуть перехопити такий сигнал та згенерувати свій. Не найнадійніша система.

Набагато надійніше системи зі змінним паролем. Сигнал із паролем від транспондера приймається блоком керування. Після розпізнавання в блоці керування генерується новий пароль та відправляється назад на транспондер. Однак і в цьому випадку зловмисники можуть перехопити такий сигнал та згенерувати свій.

У найсучасніших іммобілайзерах використовується алгоритм із шифрованим криптопаролем. У транспондері є функція шифрування. Блок управління посилає певний сигнал у транспондер, в якому потім генерується унікальний пароль, який може розпізнати тільки блок управління. Його ще називають «плаваючим» паролем. І хоча цей алгоритм надійніший, його також можна перехопити та розшифрувати.

Тому пропонується наступний простий варіант захисту. Для цього скористаємось малюнками, наведеними в [14, 15], з деякими змінами. У смарт-ключі додатково встановлюється регістр пам'яті зі зсувом та реле для автоматичного відключення живлення смарт-ключа (рис.9).

Рис.9. Смарт-ключ з доданими елементами

Регістр пам'яті зі зсувом додатково встановлюється в замок запалювання з іммобілайзером (рис.10).

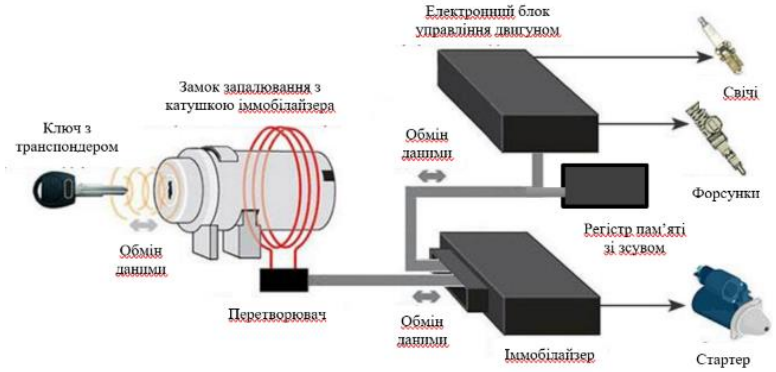

Рис.10. Схема обміну між смарт-ключом та іммобілайзером з доданим елементом

У сервісному центрі обслуговування автомобіля фахівцем центру в регістри пам'яті смарт-ключа та іммобілайзера записується набір (бажано кілька десятків) пар відповідних шифрованих кодів: в іммобілайзер код запиту, смарт-ключ з транспондером код відповіді. Слід зазначити, що водієві необхідно буде раз на два-три місяці заїжджати до центру для зміни бази кодів.

Як це працює? Процедура обміну між смарт-ключом та іммобілайзером з наступним запуском двигуна аналогічна вищеописаному (рис.1). Відмінність полягає в тому, що після виходу водія з автомобіля останній закриває автомобіль натиснувши відповідну кнопку на смарт-ключі. У цей момент з ECU надходить сигнал одночасно на регістри пам'яті смарт-ключа та іммобілайзера на зсув коду на одну позицію, після чого сигнал з ECU надходить на реле, що знаходиться в смарт-ключі, на відключення живлення смарт-ключа автоматично перерветься. Тепер, при використанні технології «Довгої руки/ключа», код смарт-ключа зловмисникам буде недоступний. У кращому випадку зловмисники зможуть зчитати код іммобілайзера, чого недостатньо для відкриття автомобіля.

Щоб здійснити поїздку, водій підходить до припаркованого автомобіля, попередньо примусово натискає спочатку кнопку включення реле на смарт-ключі, яке своїми контактами замикає ланцюг подачі живлення на смарт-ключ (перед реле у смарт-ключі додатково ставиться елемент АБО на два входи: для автоматичного підключення реле з ECU та фізичного підключення водієм натисканням відповідної кнопки на смарт-ключі). Потім водій натискає кнопку для обміну кодами з іммобілайзером. Тепер, навіть якщо зловмисники зчитають коди іммобілайзера і смарт-ключа, водій може бути спокійним тому, що після включення двигуна також відбудеться автоматична зміна кодів в іммобілайзері та смарт-ключі. Зазвичай, при включенні запалювання, іммобілайзер через

кільцеву антену, намотану навколо замку запалення на досить високій частоті запитує дані від регістру пам'яті іммобілайзера. Якщо код упізнано правильно, починається діалог між іммобілайзером та контролером. Він відбувається на низькій частоті. Якщо обмін даними завершився успішно, роботу двигуна дозволено. Найчастіше до вимкнення запалювання регістр пам'яті більше не обпитуватиметься. Після чого командою з ECU відбудеться відключення живлення смарт-ключа і база з кодами смарт-ключа знову буде недоступною.

Висновки

Розглянута методика безключового доступу до автомобіля є більш простою і більш захищеною від зловмисників в зрівнянні з розглянутими аналогами.

Література:

1. By N. Huq, C. Gibson, V. Kropotov, R. Vosseler. Cybersecurity Risk of Connected Cars URL:https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars
2. Найкращий друг викрадача – безключовий доступ. Експеримент. URL: https://autogeek.com.ua/luchshiy-drug-ugonshhika-besklyuchevoy-dostup-eksperiment/
3. Колодяжний В.М., Левтеров А.І., Малащук Є.В. Кібербезпека автомобілів: історія цифровізації автомобілів, поточний стан проблеми, цілі сталого розвитку та стандарти. *Вісник ХНАДУ*, вип. 96. 2022. С. 59-65.
4. Ivy Wigmore. Passive keyless entry (PKE). URL: https://www.techtarget.com/whatis/definition/passive-keyless-entry-PKE#:~:text=Passive%20keyless%20entry%20(PKE)%20is,touches%20the%20car%20on%20exit.
5. Keyless entry car thieves. (whichcar.com.au).
6. A. Ranganathan, S. Capkun. Are We Really Close? Verifying Proximity in Wireless Systems. URL: are_we_really_close.pdf (ethz.ch)
7. Secure Proximity Verification (Ranging)URL: https://securepositioning.com/secure-proximity-verification/.
8. A. Francillon, B. Danev, S. Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. URL:Microsoft PowerPoint - PKES_relay.pptx (ndss-symposium.org).
9. Rundgang auf DER „Autoknacker-Messe“. https://www.bild.de/auto/auto-news/diebstahl/autoklau-messe-polen-reportage-38446846.bild.html
10. Abel Valko, Relay Attack Resistant Passive Keyless Entry. Securing PKE Systems with Immobility https://www.kth.se/polopoly_fs/1.987191.1589831618!/valkoabel_47599_2869553_Relay_Attack_Resistant_Passive_Keyless_Entry-1.pdf
11. A. Francillon, B. Danev, S. Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. URL:https://eprint.iacr.org/2010/332.pdf
12. Relay Attack. URL: Relay attack - Wikipedia
13. Skybrake immobilizer: principle of operation, features, installation and dismantling. URL:https://avtotachki.com/en/immobilayzer-skybrake-princip-raboty-osobennosti-ustanovka-i-demontazh/
14. R. Verdult, Flavio D. Garcia, J. Balasch. Gone in 360 Seconds: Hijacking with Hitag2. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf
15. Principle of operation and types of engine blocking relay. https://130.com.ua/en/princip-raboty-i-raznovidnosti-rele-blokirovki-dvigatelja/