# Кібербезпека системи "Connected Car"

УДК 004.4:056.57

Підлісний Ю.І.

*Національний університет «Чернігівська політехніка», ypodlesny@ukr.net*

Сучасні електромобілі, згідно концепції "Підключений автомобіль" (Connected Car), стали частиною всесвіту "Інтернету речей" (Internet of Things, IoT), що відкриває нові можливості для покращення безпеки, комфорту, ефективності та розваг пасажирів. Більш того, з року в рік вони стають все більш автоматизованими і здатними приймати самостійні рішення в процесі їх експлуатації.

Виробники не приховують, що розумні датчики вже зараз збирають і передають інформацію про поточне GPS положення автомобіля, про стиль водіння власника, діагностичну інформацію тощо. Крім того, у виробника є можливість для віддаленого підключення авто з метою повної діагностики та оновлення програмного забезпечення, тобто, по суті, є доступ практично до всіх функцій електромобіля. Власник також має віддалений доступ до свого авто через спеціальне програмне мобільне забезпечення.

Недостатня захищеність подібних даних може призвести до потенційних ризиків. Наприклад, отримання можливості несанкційно дистанційно керувати системами автомобіля, що може привести, у залежності від цілей зловмисника, до загроз життю і здоров'ю водія та оточуючих його людей.

У зв’язку з цим існує актуальна проблема забезпечення відповідного рівня кібербезпеки сучасних електромобілів (як окремої одиниці, так й їх сукупності, що незалежно переміщуються по дорогах), тому що ще немає єдиного стандарту безпеки передавання даних від розумних датчиків електромобіля, їх шифрування та забезпечення захисту від вірогідного втручення у систему злочинців.

Основною метою дослідження був аналіз потенційних загроз та вразливостей "Connected Car" та оцінка їх впливу на стан кібербезпеки усієї системи та її складових. Це дозволило нам дослідити різноманітні потенційні загрози, зокрема атаки з використанням вразливостей пристроїв IoT, зловживання з боку користувачів і виробників, витік конфіденційної інформації тощо та у подальшому розробити та впровадити механізми контролю передачі і захисту данних, з якими оперує система.

При проведені дослідження аналізувалися наступні потенційні загрози кібербезпеці системи "Connected Car":

1) *Можливості злому систем керування автомобілем (CAN-шиною)*. CAN-шина (Controller Area Network) використовується для зв'язку між різними компонентами електромобіля, такими як двигун, гальмівні системи, системи безпеки та розваг. Злом цих систем може призвести до віддаленого контролю над автомобілем, включно з управлінням його рухом і безпекою.

2) *Виявлення вразливостей у мобільних додатках*. Багато виробників електромобілів надають мобільні додатки для управління та моніторингу автомобілем. Уразливості в цих додатках можуть дозволити зловмисникам отримати доступ до особистої інформації власників, керувати функціями автомобіля та відстежувати його місце розташування.

3) *Аналіз можливих атак на системи навігації та розваг*. Сучасні електромобілі зазвичай оснащені системами розваг і навігації, які можуть бути схильні до атак. Зловмисники можуть використовувати вразливості в цих системах для злому і отримання доступу до інших компонентів автомобіля.

4) *Забезпечення неможливості підробки оновлень ПЗ.* Виробники електромобілів регулярно випускають оновлення програмного забезпечення (ПЗ), щоб усувати вразливості та покращувати функціональність. Однак зловмисники можуть підробляти ці оновлення, щоб впровадити шкідливе ПЗ на електромобіль або зламати його системи.

5) *Захист та безпека даних, що знаходиться у системі*. Електромобілі збирають велику кількість даних про водіння, маршрути, звички користувачів тощо. Ці дані можуть бути вкрадені або скомпрометовані, якщо системи зберігання та передачі даних не захищені належним чином.

6) *Можлива наявність спеціальних закладних функцій від виробника*, які дозволяють їм здійснювати незадекларований прихований контроль через системи IoT, що може становити певну проблему з точки зору приватності та безпеки користувачів. Наприклад, виробники можуть включити в автомобілі функції, які дозволяють збирати та передавати різноманітні дані про автомобіль, його водія та пасажирів на центральний сервер без повідомлення або згоди власника автомобіля.

Проведені дослідження дозволили розробити превентивні стратегії забезпечення безпеки у системі "Connected Car".

Для вирішення виявлених потенційних загроз запропоновано застосувати такі заходи захисту, як шифрування даних, аутентифікація, мережеві фільтри та системи виявлення вторгнень для захисту пристроїв IoT та мереж, що їх обслуговують, тощо. Також представляє інтерес у застосуванні штучного інтелекту для аналізу відео і аудіо інформації, яка передається з камер відеоспостереження та інших пристроїв електромобілю без дозволу власника.

1. Songqing Chen, Chen Song, Jin-Hee Cho, Kewei Sha "Cybersecurity for Electric Vehicles: Vulnerabilities, Threats, Intrusions, and Mitigations" – 17th International Conference, WASA 2022, Dalian, China (November 24–26, 2022), Proceedings, Part II. – pp. 4-10.
2. Houbing Song, Glenn A. Fink, Sabina Jeschke "Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications" – NY: Wiley-IEEE Press, 2017 – 472 p.
3. Craig Smith "The car hacker's handbook: a guide for the penetration tester" (1st edition, March 1, 2016) – NY: No Starch Press, 2016 – 304 p.