УДК 004.056.55
О. Оробчук, Ph.D; М. Демчишин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОСНОВНІ КІБЕРЗАГРОЗИ ТА МЕТОДИ ШИФРУВАННЯ ДАНИХ ДЛЯ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ

UDC 004.056.55
O. Orobchuk, Ph.D; M. Demchyshyn

MAIN CYBER THREATS AND DATA ENCRYPTION METHODS FOR AUTONOMOUS VEHICLES

У сучасному світі автомобільні транспортні засоби (АТЗ) дедалі більше інтегруються з цифровими технологіями. В них використовують комбінацію датчиків, камер, радарів і лідарів для сканування навколишнього середовища та навігації. АТЗ створюють тривимірну карту місцевості, виявляють інші транспортні засоби, пішоходів, дорожні знаки тощо. Бортові комп'ютери використовують ці дані разом з високоточними картами для планування безпечного маршруту, керування гальмами, газом, кермом тощо. Впровадження автономних систем керування, сенсорних мереж та підключення до Інтернету відкриває нові можливості, але й водночас ця цифровізація створює нові виклики у сфері кібербезпеки, які потребують впровадження ефективних методів захисту даних.

Хакери можуть використовувати вразливості в програмному забезпеченні транспортного засобу, мережах або системах зовнішнього зв'язку [1].

Основні кіберзагрози з якими можуть стикнутися автомобільні транспортні засоби це:

1. Загрози, пов'язані з комунікаціями:

– атаки на V2V (зв'язок «транспорт-транспорт») та V2I (зв'язок «транспорт-інфраструктура»);

– перехоплення та підробка даних;

– DDoS-атаки на управління мережею.

2. Загрози для сенсорів та систем управління:

– підміна даних GPS, LiDAR, або камери, що призводить до неправильного аналізу дорожнього розташування;

– впровадження шкідливих даних у системи обробки сигналів.

3. Несанкціонований доступ до бортових систем:

– злом інтерфейсів управління;

– атаки на OTA (оновлення «по повітрю»).

4. Порушення конфіденційності даних:

– крадіжка персональної інформації, включаючи дані про маршрути.

АТЗ залежать від складних систем збору, обробки та передачі даних. Це робить їх вразливими до кібератак, які можуть порушити їх функціонування, знизити безпеку та поставити під загрозу конфіденційність. Для захисту інформації від несанкціонованого доступу запроваджено різні алгоритми, які стосуються цілісності, доступності, автентифікації та авторизації інформації на серверах, включаючи інформацію у файлах і базах даних.

Шифрування даних відіграє ключову роль у забезпеченні захисту конфіденційної інформації від хакерів і кіберзагроз. За допомогою шифрування таких критично важливих даних, як інформація про місцезнаходження, режими водіння та діагностика транспортних засобів, виробники і користувачі знижують ризик несанкціонованого доступу та потенційних кібератак [2].

Для забезпечення конфіденційності та цілісності конфіденційної інформації використовуються наступні методи захисту даних в АТЗ:

1. Криптографічні методи:

– симетричне шифрування (алгоритми: AES). Використовується для захисту даних у пам'яті автомобіля. В АТЗ симетричне шифрування зазвичай використовується через ефективність і швидкість обробки великих обсягів даних;

– асиметричне шифрування (алгоритми: RSA, ECC). Використовується для захисту ключів та зв'язку між автомобілями й інфраструктурою. Цей метод підвищує безпеку в АТЗ, дозволяючи безпечно передавати дані через загальнодоступні мережі без необхідності ділитися особистим ключем;

– хешування (алгоритми: SHA-256, SHA-3). Використовується для забезпечення цільності даних, зокрема при перевірці оновлень програмного забезпечення.

2. Протоколи захищеного зв'язку:

– використання TLS забезпечує захищений канал між транспортним засобом та хмарними сервісами, DTLS для реального часу в системах V2X;

– впровадження VPN або IPSec для мережевої ізоляції, забезпечують захист даних між транспортними засобами та серверами.

3. Безпека оновлень програмного забезпечення:

– використання цифрових підписів для перевірки справності оновлень;

– виявлення механізмів втручання під час ОТА.

4. Моніторинг та виявлення загроз:

–системи виявлення аномалій на основі штучного інтелекту (ШІ).

5. Стійкість до майбутніх загроз:

– інтеграція квантово-стійких алгоритмів шифрування.

Щоб знизити ризики, пов’язані з кібератаками, і забезпечити стабільну роботу автономних транспортних засобів потрібно дотримуватись наступних рекомендацій:

✓ Постійне оновлення систем. Регулярні ОТА-оновлення із застосуванням криптографічної верифікації.

✓ Сегментація мережі. Розділення критичних систем, таких як управління, від вторинних (мультимедіа, навігація).

✓ Моніторинг аномалій. Використання AI/ML для виявлення нетипової поведінки в системах.

✓ Залучення стандартів. Дотримання міжнародних стандартів, таких як ISO 26262, для безпеки в автомобільній галузі.

✓ Навчання користувачів. Інформування власників про важливість безпечного підключення.

Виклики щодо кіберзагроз залишаються актуальними для всіх учасників автомобільної галузі, від виробників до споживачів. Тому, автомобільні транспортні засоби вимагають комплексного підходу до кібербезпеки. Поєднання сучасних криптографічних методів, захищених протоколів зв’язку та системи моніторингу є ключем до мінімізації ризиків та забезпечення надійної роботи автономних транспортних засобів у різних умовах.

Література

1. Meyer, S.F., Elvik, R. & Johnsson, E. Risk analysis for forecasting cyberattacks against connected and autonomous vehicles. *J Transp Secur* 14, 227–247 (2021). URL: https://doi.org/10.1007/s12198-021-00236-4.
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. (2-ге видання, стереотипне). Львів : Новий Світ-2000, 2024. 678 с.