Особливістю системи впорскування автомобіля є синхронна робота форсунок відповідно до фаз газорозподілу на основі інформації від датчиків фаз.

Однак такі фактори, як нерівномірний знос компонентів двигуна і автомобіля, нестабільна якість палива і доріг, людський фактор при складанні, регулюванні та обслуговуванні автомобіля, особисті уподобання власника автомобіля і стиль водіння водія, особливо при поточних цінах на паливо і запчастини, роблять ЕБУ більш тонким для кожного конкретного випадку. Необхідно зробити попередній аналіз.

Крім того, попередній аналіз алгоритмів і програм, що використовуються в цих ЕБУ, показав, що система управління впорскуванням і запалюванням була б більш ефективною, якби в якості одного з вхідних сигналів використовувався датчик температури газу в циліндрі двигуна. Наразі такі вимірювання не реалізовані в автомобілях через відсутність датчиків, що відповідають стану двигуна внутрішнього згоряння, а збільшувати вартість автомобілів у критичній ситуації небажано.

РИЗИКИ КІБЕРБЕЗПЕКИ В МЕРЕЖЕВИХ ТРАНСПОРТНИХ ЗАСОБАХ

Біляєва В.А., Магістр
Науковий керівник – ***Біндюг С.А.,*** асистент
Харківський національний автомобільно-дорожній університет

Розвиток комунікаційних технологій вплинув на багато галузей, у тому числі й на автомобільну промисловість. Сьогодні транспортні засоби все частіше оснащуються функціями, які роблять водіння більш комфортним і безпечним для користувача. Такі системи іноді входять до базової комплектації автомобіля, а іноді встановлюються додатково. Однак із впровадженням таких технологій, окрім покращення досвіду водіння, збільшується обсяг даних, що збираються різними елементами підключеної системи автомобіля, а це означає, що персональні дані водія, власника та пасажирів можуть бути використані не за призначенням та використані не за призначенням.

Перш ніж аналізувати категорії даних, що збираються підключеними автомобілями, давайте розглянемо варіанти підключених автомобілів:

1. Транспортний засіб до транспортного засобу (V2V): бездротова система для підключення одного транспортного засобу до іншої системи, де основна роль полягає в обміні інформацією між двома транспортними засобами. Система дозволяє підключеним транспортним засобам отримувати такі дані, як швидкість, з якою вони рухаються, та місцезнаходження іншого транспортного засобу. Такі системи можуть забезпечити безпеку дорожнього руху і контролювати трафік.

2. Системи «транспортний засіб-мережа» (V2G) з'єднують транспортні засоби з електромережею, де транспортні засоби можуть бути підключені до загальної електромережі для зарядки своїх транспортних засобів і повернення надлишкової електроенергії в мережу; учасники систем V2G продають ефектроенергію в мережу в той час, коли транспортні засоби не використовуються, а ціни на електроенергію є низькими. Вони можуть заряджати свої транспортні засоби в періоди, коли ціни на електроенергію низькі.

3. Транспортний засіб-пішохід (V2P) - це система взаємодії між транспортними засобами та пішоходами (або пішохідними гаджетами), за допомогою якої транспортні засоби можуть взаємодіяти з пішоходами, що знаходяться поблизу. Отримуючи доступ до частотного діапазону смартфона, яким користується пішохід, датчики автомобіля можуть дізнатися про швидкість і напрямок руху мобільного пристрою, а отже, і пішохода.

4. Транспортний засіб до інфраструктури (V2I): системи, які з'єднують транспортні засоби з інфраструктурними ресурсами. Вона збирає дані, згенеровані транспортним засобом, і надає водієві інформацію про інфраструктуру. Ця система також працює з системами V2V і надає можливість розрахувати найкращий маршрут, допомагаючи запобігти можливим аваріям (у безпілотних транспортних засобах).

5. Транспортний засіб до хмари (V2C): технологія, яка з'єднує транспортні засоби з хмарними сервісами.

Вона створює шлях передачі даних між службами збору та зберігання даних, вбудованими в різні додатки, які користувачі підключають до своїх транспортних засобів.

На даний момент більшість таких систем підключення існують в основному тільки в транспортних засобах, обладнаних автопілотом, але в найближчому майбутньому можуть бути впроваджені у всіх транспортних засобах і їх екосистемах. І в такому випадку в майбутньому, прокладаючи свій наступний маршрут на Google Maps, ви неодмінно будете знати, що з-за рогу вашого будинку вискочить людина і вам потрібно буде трохи пригальмувати, щоб не потрапити в аварію.

Однак важливо пам'ятати, що таке розширення спектру систем зв'язку між зовнішнім світом і автомобілем також підвищує рівень загрози злому автомобіля і вилучення персональних даних або відключення системи автопілота, що може призвести до аварії. Середньостатистичний підключений автомобіль зберігає та обробляє величезну кількість даних (наведена нижче класифікація даних не обов'язково є повною, а можливість збору та обробки певного набору даних залежить від того, які системи та сервіси в автомобілі підключені):

- Дані про рух транспортного засобу (швидкість, пройдений шлях, місцезнаходження транспортного засобу);

- Дані про стан транспортного засобу (стан двигуна, температура, тиск у шинах);

- Біометричні дані власника автомобіля та водія (наприклад, відбитки пальців, необхідні для доступу до салону автомобіля);

- Персональні дані власника автомобіля (документи, пов'язані з автомобілем, платіжні дані для додатків, що використовуються в автомобілі);

- Дані смартфона, водія та пасажирів, зібрані під час підключення стартфона до автомобільної системи;

- дані, отримані під час аудіо-/відеофіксації навколишнього середовища (наприклад, при використанні відеопаркувальних датчиків, при встановленні відеореєстратора в автомобілі).

Існує також ще одна група даних, отриманих з підключених автомобілів, яка класифікується як «дані, що свідчать про кримінальні або інші правопорушення». Це будь-які дані, які збирає автомобіль і які набувають такого статусу з самого початку його використання.

Наприклад, набір даних про швидкість або місцезнаходження транспортного засобу не є даними, що мають відношення до виявлення правопорушення, доки вони не будуть використані для таких цілей. Така інформація може допомогти поліції ідентифікувати водіїв, які порушують правила дорожнього руху, або підтвердити алібі підозрюваного правопорушника.

Персональні дані повинні використовуватися з цією метою лише в межах юрисдикції уповноважених державних органів, без порушення прав і свобод осіб, яких стосується інформація, та відповідно до законодавства країни, в якій необхідне використання інформації.

Деякі з вищезазначених видів інформації не стосуються безпосередньо особи водія/пасажира або власника транспортного засобу,

Вони все одно класифікуються як персональні дані. Найпростішим прикладом є дані про географічне розташування транспортного засобу, які дозволяють особам, відповідальним за обробку таких даних, дізнатися про конкретні звички та вподобання водія/власника транспортного засобу. Наприклад, часта присутність автомобіля біля церкви релігійної організації може свідчити про приналежність водія до певної релігійної групи, або постійна присутність автомобіля біля закладу відповідної тематики може свідчити про сексуальну орієнтацію водія/власника.

Транспортний засіб набуває статусу «підключеного автомобіля», якщо в ньому встановлено спеціальне програмне забезпечення, яке підключає його до різних систем зв'язку та телекомунікацій. Наприклад, автомобілі, обладнані системами ADAS (Advanced Driver Assistance Systems).

- Радари ближнього та дальнього радіусу дії
- зовнішні та внутрішні відеокамери
- Паркувальний радар
- Лазерний далекомір (LIDAR - Light Identification Detection and Ranging);
- Адаптивне управління світлом.
- Адаптивний круїз-контроль.

Такі системи збирають дані, пов’язані з рухом транспортного засобу та відеозаписами навколишнього середовища. Схожим методом отримання інформації є відео/фотозйомка в громадських місцях. Такі дані вважаються персональними і повинні використовуватися одержувачем і контролером даних відповідно до законодавства країни, де знаходиться транспортний засіб, не порушуючи при цьому права і свободи людини.

У 2016 році Міжнародна автомобільна федерація (FIA) запустила в Європі кампанію «Мій автомобіль, мої дані». Її мета - допомогти автовласникам зрозуміти свої права щодо персональних даних. Вона вважає, що для забезпечення прозорості та релевантності збору та обробки даних автомобільною системою необхідно

- Впровадити спеціальну систему попередження в транспортних засобах, яка дозволить користувачам знати, які дані передаються до служби збору та обробки даних;

- надати можливість власникам автомобілів безпосередньо обирати дані, які будуть передані службам збору та обробки даних, через інтерфейс автомобіля;

- зобов’язати автовиробників створювати безпечні, стандартизовані, багатоплатформні платформи для забезпечення відкритого доступу до даних про транспортні засоби для різних постачальників послуг. Прецедентом обов’язкового використання технологій для підключених автомобілів на законодавчому рівні є ініціатива e-Call. Ця програма була розроблена в Європейському Союзі для підвищення безпеки користувачів автомобілів і включає в себе наступне

Програма включає набір датчиків та програмне забезпечення, призначене для оповіщення служби порятунку 112 у разі автомобільної аварії, передачі координат транспортного засобу та надання допомоги водієві та пасажирам у найкоротші терміни. у 2018 році ініціатива e-Call була відповідний мандат. Існує «Робочий документ щодо впровадження захисту даних та конфіденційності в системі ініціативи e-Call», який визначає принципи e-Call як сервісу збору даних, а також «Керівні принципи обробки персональних даних в контексті підключених автомобілів та пов’язаних з ними додатків». У них є розділ, присвячений цій ініціативі.

З дозволу користувача додаток може отримувати персональні дані, такі як дані про автомобіль і ДТП, номери страхових полісів і паспортні дані, щоб допомогти прискорити надання допомоги, перевірити членство в автоклубі і запобігти проблемам, пов’язаним з мовним бар’єром.

Згідно з положеннями нормативно-правових актів, що стосуються цієї ініціалтиви, е-дзвінок збирає дані постійно, але передає їх лише тоді, коли додаток активовано.

Хоча цей механізм повністю виправданий принципом безпеки персональних даних, який полягає в мінімізації збору та обробки, оскільки додаток не передає дані за межі автомобільної системи, поки вони не будуть потрібні, той

факт, що деякі дані все ще зберігаються в автомобілі, створює певні ризики. створює певні ризики.

Оскільки кількість датчиків, програмного та апаратного забезпечення в транспортних засобах продовжує зростати, зростає і кількість вразливостей, через які вони можуть бути зламані. Не слід забувати, що транспортні засоби є джерелом підвищеної небезпеки, і що злом навігаційної системи автомобіля, який рухається на автопілоті, може мати дуже сумні наслідки. Тому до захисту систем від злому слід ставитися з особливою ретельністю. Уряд Великої Британії опублікував інструкцію «Принципи кібербезпеки в підключених і автоматизованих транспортних засобах». З цього посібника можна виділити вісім ключових принципів для досягнення належного рівня кібербезпеки в підключених автомобільних системах:

1. Питання організаційної безпеки повинні вирішуватися на рівні корпоративної ради

2. Ризики безпеки повинні оцінюватися і управлятися належним чином; і

3. Компанії повинні забезпечити службу підтримки, включаючи реагування на інциденти безпеки, щоб гарантувати, що системи захищені протягом усього періоду їх існування

4. Всі компанії, включаючи субпідрядників, постачальників та потенційних третіх осіб, повинні працювати разом над покращенням безпеки своїх систем

5. Системи безпеки повинні бути розроблені з використанням багаторівневої технології

6. Безпека програмного забезпечення повинна гарантуватися протягом усього життєвого циклу програмного забезпечення: 7:

7. Процеси зберігання та передачі даних повинні бути безпечними та контрольованими

8. Системи повинні бути стійкими до атак і спроектовані таким чином, щоб реагувати належним чином у разі збоїв у системі безпеки або датчиків: 9:

Дотримання цих принципів автовиробниками, виробниками програмного та апаратного забезпечення забезпечить користувачам безпечну експлуатацію підключених автомобільних систем та захист їхніх персональних даних.