УДК 536.24

РИЗИКИ КИБЕРБЕЗПЕКИ ДЛЯ ПІДКЛЮЧЕНИХ ДО МЕРЕЖІ АВТОМОБІЛІВ

Симбірський Г. Д.
Харківський національний університет радіоелектроніки

Розвиток комунікаційних технологій впливає багато виробничі галузі, зокрема і автомобільну промисловість. На сьогоднішній день, автомобіль обростає все більшим і більшим функціоналом, який покликаний зробити його експлуатацію комфортнішою та безпечнішою для користувача. Такі системи можуть входити до комплектації автомобіля або встановлюються в машину додатково. Але з впровадженням таких технологій, окрім покращення процесу їзди, збільшується і кількість даних, які збираються різними елементами системи підключеного автомобіля, а отже, і кількість персональних даних водія, власника, пасажира, які можуть потрапити не в ті руки та використовуватися не за призначенням.

Перед аналізом питання, які категорії даних збирає підключений автомобіль, розглянемо варіанти підключень автотранспортних засобів:

1. V2V (Vehicle-to-vehicle), бездротова система підключення одного автомобіля до іншого система, головне завдання якої – обмін інформацією між двома автомобілями. З її допомогою, підключений автомобіль може отримувати дані про швидкість руху, місцезнаходження іншого автомобіля. Подібні системи здатні забезпечувати безпеку та контролювати трафік на дорогах.

2. V2G (Vehicle-to-grid), система підключення автомобіля до енергосистем, що дозволяє підключати автомобілі до загальної електричної мережі для підзарядки машини або повернення зайвої електроенергії назад до мережі. Учасники системи V2G зможуть продавати електроенергію в енергосистему – у ті години, коли машина не використовується, і заряджати автомобіль у години, коли електроенергія дешевша.

3. V2P (Vehicle-to-pedestrian) - система взаємодії автомобіля з пішоходами (а точніше їх гаджетами), через яку автомобіль може взаємодіяти з пішоходами, що знаходяться в безпосередній близькості від нього. Отримуючи доступ до частотного діапазону смартфонів, якими користуються пішоходи, сенсори автомобіля можуть дізнатися швидкість та напрямок руху мобільного пристрою, а значить, і пішохода.

4. V2I (Vehicle to Infrastructure), система підключення автомобіля до ресурсів інфраструктури: збирає дані, які виробляє автомобіль та надає інформацію про інфраструктуру водію. Дана система працює в комплексі із системами V2V і так само забезпечує можливість прорахунку найоптимальнішого маршруту та допомагає запобігти можливим ДТП (в автомобілях з автопілотом).

5. V2C (Vehicle to Cloud), технологія підключення автомобіля до хмарних сервісів, що створює канал передачі даних між автомобілем і сервісами збору та зберігання даних, вбудованими в різні програми, які користувач підключає до автомобіля.

Поки що більшість із цих систем підключень присутні в основному тільки в автомобілях, в яких є автопілот, але не виключено, що незабаром вони обов’язково впроваджуватимуться у всі автомобілі та їх екосистеми. І в такому разі в майбутньому при побудові чергового маршруту на сервісі Google Maps ви точно знатимете, що з-за рогу будинку зараз вибіжить людина, і вам слід трохи зменшити швидкість свого автомобіля, щоб не потрапити в ДТП. Але не варто забувати, що з подібним розширенням спектра систем зв’язку зовнішнього світу з автомобілем зростає і рівень загроз злому вашого автомобіля і вилучення з нього ваших персональних даних або приведення в непридатність систем автопілота, що може призвести до ДТП.

Середньостатистичний підключений автомобіль накопичує та обробляє величезний обсяг даних (наведена нижче класифікація даних не обов’язково є повною, а функція збору та обробки тієї чи іншої групи даних залежить від того, які системи та сервіси підключені в автомобілі):

• дані про пересування автомобіля (швидкість, подолана відстань, геолокація автомобіля);

• дані про стан автомобіля (стан двигуна, його температура, тиск у шинах);

• біометричні дані власника авто, водія (наприклад, відбиток пальця, який потрібен для доступу в салон транспортного засобу);

• персональні дані власника автомобіля (його документи, прив'язані до автомобіля, дані про оплату додатків, що використовуються в авто);

• дані зі смартфона, водія, пасажира, зібрані за його підключення до системи автомобіля;

• дані, які отримуються при аудіо/відео фіксації оточення (наприклад, під час використання відео парктроників, установки чорної скриньки в авто).

Існує і окрема група даних, отриманих із підключених автомобілів, класифікована як "Дані, які розкривають кримінальні злочини та інші порушення". Це можуть бути будь-які дані, зібрані автомобілем, і такий статус вони набувають від початку процесу їх використання. Так, наприклад, сукупність даних про швидкість і розташування автомобіля не є даними, пов'язаними з розкриттям злочинів, до початку їх використання в подібних цілях. Така інформація може допомогти поліції викрити водія у порушенні правил дорожнього руху або підтвердити алібі водія, підозрюваного у скоєнні кримінального злочину.

Персональні дані повинні використовуватися з цією метою лише під юрисдикцією уповноваженого державного органу, при цьому не порушуючи права та свободи особи, до якої ці дані належать і відповідно до законодавства держави, в якій потрібне використання цих даних.

Незважаючи на те, що деякі з перерахованих видів інформації безпосередньо можуть і не відносяться до особи водія/пасажира або власника авто, вони все одно можуть відноситись до категорії персональних даних. Найпростіший приклад: за даними, пов'язаними з геолокацією автомобіля, особа, відповідальна за обробку таких даних, може дізнатися про деякі звички та переваги водія/власника автомобіля. Наприклад, часте розташування автомобіля біля храму тієї чи іншої релігійної організації може розкрити приналежність водія до певної релігійної громади, а постійні появи авто біля

закладів відповідної тематики можуть вказати на сексуальну орієнтацію водія/власника автомобіля.

Автомобіль набуває статусу підключеного у разі встановлення в нього спеціального програмного забезпечення (далі ПЗ) пов'язаного з різними системами комунікації та зв'язку. Наприклад, підключеним можна вважати автомобіль, оснащений ADAS (Advanced Driver Assistance Systems – просунуті системи допомоги водієві), які включають:

• радари ближньої та далекої дії;

• зовнішні та внутрішні відеокамери;

• паркувальні радари;

• лазерні далекоміри (LIDAR - Light Identification Detection and Ranging - світлове виявлення та визначення дальності);

• адаптивне керування світлом;

• адаптивний круїз-контроль.

У таких системах збираються дані, пов'язані з пересуваннями автомобіля, та відео фіксацією його оточення. Подібний спосіб отримання інформації пов'язаний із відео/фотозйомкою у громадських місцях. Такі дані відносяться до персональних даних та повинні використовуватися одержувачами та контролерами даних, не порушуючи права та свободи людини, та згідно із законами держави під юрисдикцією якої знаходиться автомобіль.

У 2016 році FIA (The Fédération Internationale de l'Automobile – Інтернаціональна Федерація Автомобілістів) розпочала в Європі кампанію названу "Мій автомобіль – мої дані". Мета - допомогти власникам автомобілів розібратися у своїх правах, пов'язаних із персональними даними. Вони вважають, що для забезпечення прозорості та адекватності збору та обробки даних системами автомобіля потрібно:

• Ввести спеціальні системи оповіщення в автомобілі, які дозволять користувачеві знати, які дані передаються в послуги збору та обробки даних;

• Дозволити власнику автомобіля безпосередньо за допомогою інтерфейсу авто вибирати які дані він хоче передавати до сервісів збору та обробки даних;

• Зобов'язати виробників автомобілів створювати захищені, стандартизовані, мультиплатформні майданчики для можливості

відкритого доступу різних постачальників послуг до даних автомобіля. Існує прецедент, коли використання технологій для підключеного автомобіля стало обов'язковим на законодавчому рівні, а саме ініціатива e-Call. Ця програма була створена в Європейському Союзі, з метою збільшити безпеку користувачів транспортних засобів, дана програма включає сукупність датчиків і ПЗ, покликаних у разі пошкодження автомобіля внаслідок аварії викликати службу 112 передаючи їй координати автомобіля, для якнайшвидшого надання допомоги водію та пасажирам автомобіля . У 2018 ініціатива e-Call стала обов'язково впроваджуватися у всі легкові автомобілі. Існує "Робочий документ про захист даних та впровадження конфіденційності в систему ініціативи e-Call", яким визначаються принципи функціонування e-Call як сервіс, що застосовує збір даних, так само даній ініціативі присвячений розділ у "Посібнику з обробки персональних даних у контексті підключених автомобілів та пов'язаних з ними додатків". З дозволу користувача дана програма може отримувати дані як про автомобіль та ДТП, так і свої особисті дані, наприклад номер страхового поліса, паспортні дані для прискорення процесу надання допомоги, перевірки приналежності до клубів автомобілістів, запобігання проблемам, пов'язаним з мовним бар'єром. Виходячи з положень нормативно-правових актів пов'язаних з даною ініціативою e-Call збирає дані безперервно, але передає їх тільки в момент коли додаток активується, подібний механізм повністю виправданий принципом безпеки персональних даних а саме мінімізації збору та обробки, так як ця програма не виводить дані за межі системи автомобіля до того моменту поки в цьому немає потреби, але той факт, що деякий обсяг даних все одно зберігається в автомобілі створює певні ризики для користувачів.

Через постійне збільшення сенсорів, ПЗ та обладнання в автомобілях збільшується і кількість вразливостей, які можуть спричинити злам автомобіля. Не варто забувати, що машина - це джерело підвищеної небезпеки, і зламування системи навігації в авто, керованому автопілотом, може призвести до дуже сумних наслідків, тому до питань захисту його систем від злому слід ставитися з максимальною серйозністю. Уряд Великобританії випустив керівництво про "Принципи кібербезпеки в підключених та автоматизованих

транспортних засобах". З цього керівництва можна підкреслити 8 основних принципів для створення належного рівня кібербезпеки в системах підключених автомобілів:

1. Питання з організаційної безпеки повинні просуватися на рівні правління компанії;

2. Ризики безпеки повинні оцінюватися та керуватися належним чином;

3. Компаніям необхідно надавати сервісне обслуговування, що включає реагування на інциденти, пов’язані з загрозами безпеці, щоб забезпечити захист систем протягом усього терміну їх служби:

4. Всі компанії, включаючи субпідрядників, постачальників та потенційних третіх осіб, повинні працювати разом для підвищення безпеки системи:

5. Системи захисту повинні бути розроблені з використанням технології багатошарової:

6. Безпека ПЗ повинна бути гарантована на весь термін його експлуатації:

7. Процеси зберігання та передачі даних повинні бути безпечні та мати можливості контролю над ними:

8. Система повинна бути розроблена таким чином, щоб вона була стійкою до атак та реагувала відповідним чином у разі відмови її захисту або датчиків:

Виконання цих принципів виробниками автомобілів, ПЗ та обладнання може гарантувати користувачам безпеку експлуатації систем підключених автомобілів та надійний захист їх персональних даних.