КІБЕРБЕЗПЕКА В АВТОМОБІЛЬНОМУ ТРАНСПОРТІ

Мельник Б.О., ст. гр. М-13-21,
керівник доц. каф. ІПМ Шевченко В.О.
ХНАДУ

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення інформаційно-комунікаційних технологій (ІКТ) та інформаційно-телекомунікаційних систем (ІТС). Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки.

Кібербезпека транспорту – безпека особистих даних, якими користувач ділиться з транспортним пристроєм чи агрегатором транспортних даних. Сьогодні «розумні» системи оточують нас усюди: вони контролюють траси та залізниці за допомогою платформ для моніторингу, відстежують та запобігають заторам як навігатори, відповідають за безпеку пасажирів та водія всередині автомобілів.

Всі ці системи використовують контролери та датчики, які дозволяють тримати зв’язок із зовнішніми джерелами даних. На практиці виявляється, що чим більше у транспортного засобу зв’язку із зовнішнім світом, тим уразливіше для кібератак ззовні він стає і тим більше йому потрібна спеціальна система захисту.

У автомобілебудуванні всерйоз взялися за кібербезпеку і почали інвестувати в проектування та розгортання кіберзахисних рішень приблизно шість років тому. Сьогодні в автомобільній індустрії кібербезпека забезпечується як апаратними, так і програмними рішеннями, але потрібно пройти довгий шлях, перш ніж всі до одного ECU (електронні блоки управління) в машині будуть захищені від кібератак, що зараз активізуються.

Кібербезпека в автомобілебудуванні набагато складніша, ніж на смартфонах та ПК, з двох основних причин:

1. Десятки ECU в кожній машині, з’єднані безліччю електронних шин і відповідають за різні швидкості та характеристики, та

2. Багато потенційних точок доступу, як розташованих всередині автомобіля, так і віддалених, зокрема, OBDII, USB і SD-порти, безключовий доступ, Bluetooth і Wi-Fi, вбудований модем, датчики, інфотейнмент або програми для смартфонів, а також безліч підключень з застосуванням телематики та інших хмарних систем, що мають доступ до систем автомобіля.

У 2015 році дослідники Чарлі Міллер та Кріс Валасек стурбувалися питаннями кібербезпеки та стали досліджувати цю тему на автомобілі марки Jeep. У результаті вони знайшли вразливість у телематичному навігаційному блоці, за допомогою якого дистанційно «залізли» всередину автомобіля та розшифрували повідомлення, які ходили захищеною мережею. Міллер і Валасек змогли віддалено взяти керування автомобілем на себе: почали балуватися вікнами та двірниками, а потім взагалі скинули машину в кювет. Вони могли регулювати швидкість і крутити кермо: це був перший серйозний публічний кейс - після нього автопромисловість почала дивитися на кібербезпеку серйозніше.

Технічно ми можемо уявити собі ситуацію, в якій машина їде швидкісною трасою і їй віддалено вимикають двигун або керування. Чисто теоретично хакер може віддалено перехопити керування у водія, що сидить за кермом. Лякатися, однак, не варто: зробити це вдасться далеко не з кожним автомобілем - все залежить від того, наскільки вразлива електроніка всередині машини.

У 2022 році хакер, який знайшов «ключ» до телематичного блоку, не зможе керувати кермом та гальмами. Раніше блоки всередині автомобіля працювали через центральну шину; зараз вони розділені між собою за функціями і можуть залежати один від одного тільки в їх рамках - без взаємодії з центральною віссю.

Автомобільна кіберзлочинність зростає загрозливими темпами. Наприклад, у Лондоні позаминулого року зловмисники, зробивши дублікат радіобрелка для розблокування іммобілайзера, викрали понад 6000 автомобілів. Кількість викрадень з використанням високотехнологічних засобів збільшується пропорційно до того, як машини «розумніють».

Викрадення машин – вигідний бізнес для всього ланцюжка залучених до неї людей. Саме тому професійні викрадачі мають інструменти і техніку, вартість якої часом досягає декількох мільйонів гривень. З такою допомогою доступно багато чого:

- Клонування електронного ключа – один із найчастіших випадків викрадення. Більшість нових машин обладнано іммобілайзером. Це захисна система, що блокує рух до отримання сигналу від вбудованого в ключ чіпа. Щоб завести автомобіль, потрібно просто зробити дублікат брелока. Робиться це за дві-три хвилини, після чого автомобіль спокійно їде «в нікуди». У зоні ризику — безліч марок і моделей. Ця штатна система захисту потребує додаткового допрацювання;

- Пульт дистанційного відкриття дверей – щастя для автокрадія. Майже всі нові автомобілі продаються із ключами, доповненими кнопками для відкриття та закриття машини. Пульт надсилає не захищений сигнал. За допомогою спеціального приладу – кодграбера цей сигнал уловлюється і у злочинця з'являється можливість спокійно поринути у салон. "Розумні" машини, підключені до смартфону, теж знаходяться у зоні ризику. Власник за допомогою програми на телефоні дистанційно керує деякими функціями автомобіля. Він може запустити двигун, відкрити двері, привести в роботу частину вузлів та агрегатів, контролювати характеристики техніки. Просто так зламати програму смартфона не вдасться, і перехопити сигнал теж. Але якщо заразити телефон вірусом, хакер отримає доступ до управління нарівні з власником.

Найголовніше при виявленні кібератаки - вчасно зупинити її розповсюдження всередині автомобіля. На жаль, більшість сигналізацій не є перешкодою для досвідчених викрадачів. Наприклад, заводський захист, сигналізація з дистанційним відкриттям дверей або з динамічним кодом нічим не краща за штатний пульт. Код перехоплюється тим самим кодграбером, і машина з легкістю відкривається, заводиться і їде.

Та все ж Чарлі Міллер та Кріс Валасек, які зламали Jeep Cherokee, на конференції Black Hat представили недорогий пристрій, який може протистояти атакам хакерів на систему авто. Собівартість такого пристрою становить 150 дол. Воно складається із звичайної

панелі та мікроконтролера NXP. Пристрій підключається до роз'єму під машиною або до приладової панелі (порт OBD2). Пристрій спочатку фіксує характерні параметри автомобіля, але якщо його переключити в режим виявлення, воно виявить аномалії, що відрізняються від стандартної поведінки машини.

Комерційний сектор також розробляє рішення щодо боротьби з кіберзлочинцями: Наприклад, у 2019 році компанія Jaguar Land Rover уклала співпрацю BlackBerry і почала використовувати їхній софт для кібербезпеки у всіх своїх нових автомобілях. За умовами співпраці BlackBerry також допомагає виявляти потенційні вразливості у системах безпеки транспортних засобів, у тому числі у безпілотниках.

Тобто розробки активно ведуться і є певні успіхи. Можливо, найближчими роками всі автомобілі будуть випускатися із системами захисту від хакерського злому. Але що робити власникам сучасних машин зараз?

Купуючи нове авто, необхідно дізнатися, яке електрообладнання і бездротові системи в ньому встановлені. Потрібно знати всі гаджети, що є в машині. При покупці б/у автомобіля обов'язково потрібно заїхати до кваліфікованого електрика, щоб він перевірив весь електроланцюг та виявив наявність додаткового обладнання.

Купувати машину потрібно лише у перевірених автодилерів. Ремонт авто також потрібно здійснювати на перевірених СТО. Горе-ремонтники можуть маніпулювати комп'ютерними системами.

Необхідно захищати важливу інформацію. Якщо в машині встановлена якась система безпеки, то компанія-розробник надає цінну інформацію з управління або розблокування системи та всі необхідні паролі. Ці документи слід зберігати в надійному місці, не можна їх залишати в машині.

Слід бути обережним при покупці автозапчастин та різних пристроїв. Електроприлади, що продаються на ринку, рідко проходять ретельну перевірку або випробування. Якщо встановити такий пристрій, підвищиться вразливість автомобіля.

Бажано знайти кваліфікованого спеціаліста, який стежитиме за оновленням ПЗ або пояснить автовласнику, як це робити.

Слід встановлювати або оновлювати програмне забезпечення лише згідно з рекомендаціями автовиробника.

Важливо приділяти особливу увагу вибору додатків, устаткування чи програм, що вимагають зміна коду ПЗ. Не варто завантажувати неперевірені програми, зокрема музику.

Потрібно не допускати сторонніх осіб та невідомі пристрої до діагностичного порту автомобіля (OBD-II). Зазвичай він розташований з боку водія під панеллю приладів. Через цей порт можна отримати доступ до всіх систем автомобіля.

Не варто передавати смартфони та планшети стороннім особам.

Як би це дивно не звучало, але найефективніші засоби захисту від крадіжки - механічні блокатори. З ними викрадачі намагаються не зв'язуватися. Навіщо витрачати сили та привертати увагу на таке трудомістке завдання, коли можна легко, швидко та безшумно зламати будь-яку електронну оборону.

Кількість автономного транспорту настільки мала, що випадків викрадення повністю без фізичного контакту поки що зафіксовано не було. Але й сучасна техніка перебуває у зоні ризику. Так, змусити її виїхати в сусіднє місто не вдасться, але втрутитися у роботу деяких агрегатів та електронних систем – просто.

Насправді надійно захиститися від атак хакерів на автомобіль можна тільки одним способом - їздити на стареньких «Жигулях», в яких немає електроніки. Такі автомобілі точно ніхто не зламає.

Але ж сучасна людина звикла до комфорту, тому і використовує автомобілі, напхані електронікою. У цьому випадку потрібно дотримуватися вищенаведених порад і при появі надійної системи захисту придбати її та встановити на свій автомобіль. Але варто визнати, що навіть це не гарантує повний захист від хакерського злому.

Література

1. https://habr.com/ru/company/macloud/blog/564054/
2. https://trends.rbc.ru/trends/industry/614041579a79471ac5adba05
3. https://эксперт-авто43.рф/avtomobilistu/mogut-li-hakery-distantsionno-ugnat-mashinu.html