# ПРОБЛЕМИ ЗАХИЩЕНОСТІ КОМПОНЕНТІВ СУЧАСНОГО АВТОМОБІЛІВ ВІД КІБЕРАТАК

Фесенко Д. О.
Науковий керівник – проф., Халімов Г.З.
Харківский національний університет радіоелектроніки
(61166, Харків, проспект Науки, 14, каф.Безпеки інформаційних технологій. Тел.702-14-25)
e-mail: dmytro.fesenko@nure.ua

Nowadays automotive industry has need in development of additional methods that would improve security of auto systems to achieve much more proficient security and trust levels. For this full understating of threads that would lead to improper operations with car components is needed, to understand what could cause road accidents or driving away of a vehicle.

Автоіндустрія потребує наразі розроблення додаткових методів захисту компонентів транспортного засобу та розроблення комплексних засобів захисту для систем авто для підвищення рівня захищеності та довіри, для цього необхідно розглянути можливі загрози, що могли б спричинити неправильну роботу компонентів автомобіля і як наслідок – привести до дорожньо-транспортної пригоди чи викрадення транспортного засобу.

Більшість сучасних транспортних засобів має на борту мультимедійну систему, яка дозволяє використовувати його як повноцінний персональний комп'ютер з можливістю виходу в мережу інтернет через вбудований модем, який підтримує використання SIM-карт для доступу до GSM мереж та вбудованим Wi-Fi модулем 802.11/n. Це дає можливість використання більш зручних та високотехнологічних засобів, що дозволяють користувачу отримувати інформацію про стан вузлів авто в режимі реального часу, дивитись фільми або працювати з іншими даними та навіть передавати їх по P2P мережі автомобіля. В той же час використання таких технологій можливість хакерських атак на системи авто для перехоплення даних, їх підміни та компрометації роботи систем та вузлів транспортного засобу через збільшення кількості атак даного виду в останній час. Данні атаки є можливими через використання давно відомих технологій, для яких виявлено багато вразливостей, які переходять до нових розробок від старих, наприклад багато мультимедійних систем використовує в якості операційної системи ОС Android, часто не останніх версій.

Мультимедійна система автомобіля з'єднана з іншими найчастіше через мережу CAN, що дозволяє зробити більш легким та ефективним з'єднання електричних елементів транспортного засобу, але в той же час на даний протокол з'єднання розроблено багато атак, які оновлюються з апгрейдом захищеності протоколу.

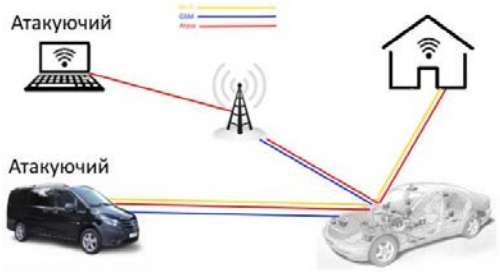


Рисунок 1 – Схема бездротових з`єднань авто з мережею інтернет

Розглянемо вид атак, що направлений на отримання керування пристроями автомобілю дистанційно. На рисунку 1 представлено приклад з'єднання мультимедійної системи з мережею інтернет через різні бездротові канали зв'язку через які можливі атаки на мережі, як підтримуються даним транспортним засобом – це мережа Bluetooth, вектором атаки який використовує помилки реалізації протоколу та дозволяє виконати атаку спарювання пристрою атакуючого з пристроєм встановленим на авто Wi-Fi мережу, яка найчастіше буде використовуватися для доступу до мережі інтернет з метою серфінга інтернет сторінок, оновлення навігаційних карт. Тут атаки можуть бути різноманітні: від реалізації атаки на стек до можливостей проведення Fake AP/MITM атаки. В разі успішно проведеної атаки атакуючий отримує доступ до компонентів транспортного засобу, що дозволяє йому керувати ними в своїх цілях.

Виходом з ситуації може бути розроблення комплексної системи захисту інформації для сучасного транспортного засобу, що є надзвичайно важливим етапом для покращення захищеності життя водія та пасажирів, оскільки під час створення такої системи проводиться обстеження всіх середовищ функціонування ІТС та розглядаються всі можливі варіанти взаємного впливу елементів різних середовищ на безпеку системи.