УДК 004.056

А.А. КОЗЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

АНАЛИЗ ПОВЕРХНОСТИ АТАКИ НА СОВРЕМЕННЫЕ АВТОМОБИЛИ

Современные автомобили уже давно не просто средство для передвижения. Встроенные в них сервисы предоставляют пользователям широкие возможности: от подогрева сидений до заказа билетов в театр. Вместе с развитием потребительских сервисов развивались также системы и сервисы, обеспечивающие безопасность водителя [1]. Однако, подобные решения, призванные повысить удобство вождения и сделать его более безопасным, архитектурно основаны на технологиях и алгоритмах, которые сами по себе несут угрозы информационной безопасности [2]. Внедрение новых технологий в автомобилестроение, порой без должного внимания к информационной безопасности, влечет за собой рост способов реализации угроз безопасности [3]. В докладе для каждого из доменов ИБ: физического, локального и удаленного, обсуждаются поверхность атаки и возможности потенциальных злоумышленников. В заключении рассматриваются способы обеспечения безопасности современных автомобилей, а также обозначаются открытые вопросы.

Основываясь на внутренней технической оснащенности и функциональных возможностях, без ограничения общности разделить все автомобили на три категории:

- Устаревший автомобиль
- Классический автомобиль
- Современный автомобиль

В контексте анализа безопасности автомобилей следует разделять всех злоумышленников по двум атрибутам:

- наличие ресурсов (деньги, время)
- наличие профильных технических знаний.

Из такой аналитической позиции видна тенденция снижения порога вхождения в область информационной безопасности автомобилей. В основном - за счет удешевления аппаратных инструментов воздействия и архитектурной схожести автомобиля с уже хорошо изученными объектами ЛВС. Кроме того, сами автомобили стали более доступными для исследования. Если раньше автомобиль был предметом роскоши, то сейчас он есть почти в каждой семье.

Тренд снижения порога вхождения неразрывно связан с еще одним трендом – изменения объектов воздействия внутри автомобиля. В соответствии с картой потоков данных автомобиля, всего можно выделить три типа информационных доменов:

- физический (требуется физический контакт с объектом, например, шина CAN)
- локальный (adjacent) (взаимодействие возможно в пределах до 100 м, например, WiFi)
- удаленный (взаимодействие возможно на расстоянии много большим 100 м от объекта, например, GSM).

В настоящее время вопросом обеспечения безопасности действительно озаботились государственные регуляторы, автомобильные вендоры и компании в области информационной безопасности Каждый из них в рамках своих полномочий вносит свой вклад в обеспечение безопасности автомобильной индустрии. Их скоординированные усилия в области информационной безопасности обеспечивают снижение вероятности реализации угроз безопасности, достигаемое различными методами, направленными на:

- уменьшение поверхности атаки
- повышение сложности реализации компьютерной атаки
- повышение скорости реагирования на инциденты ИБ

Открытые вопросы включают в себя:

- разработку новой архитектуры ЛВС и ЭБУ автомобиля, ориентированной на безопасность (Security by Design)
- разработку новых моделей событий безопасности на основе доступных данных через TCU автомобиля

Список литературы

1. Мардоян Гурген Робертович, Симонян Рубен Игоревич, Карпов Никита Андреевич, Пронин Николай Александрович, Метелев Сергей Юрьевич Современные подходы к испытанию систем ADAS на всех этапах разработки // Труды НГТУ им. Р.Е. Алексеева. 2018. №4 (123).

2. Клиновенко В.В., Колистратов М.В. Автомобильная электроника и угроза ее информационной безопасности // E-Scio. 2021. №9 (60).

3. Скатков Александр Владимирович, Брюховецкий Алексей Алексеевич, Моисеев Дмитрий Владимирович, Воронин Дмитрий Юрьевич. Обеспечение безопасности интеллектуальных транспортных средств в инфраструктуре умного города // International Journal of Open Information Technologies. 2020. №11.