

(Слайд 1) Здравствуйте, уважаемые члены экзаменационной комиссии! Вашему вниманию предлагается выпускная квалификационная работа на тему – **«Анализ информационной безопасности современного автомобиля»**.

(Слайд 2) Цель выпускной квалификационной работы - повышение информационной безопасности автомобиля путем анализа возможных угроз и перспективных методов защиты информационных систем.

Достижению цели способствовали задачи исследования, представленные на слайде презентации.

(Слайд 3) На рисунке показана типичная топология автомобильной сети с оптимальной защитой. К сожалению, не все коммуникации, обозначенные как безопасные, всегда верны. Как можно видеть, сеть состоит из нескольких сетей. Ethernet использует систему ADAS, систему помощи водителю. Это набор определенных алгоритмов, которые в разной степени помогают водителю в быстром принятии решений для безопасного и легкого управления транспортным средством. Компьютерная диагностика автомобиля — это диагностика различных систем автомобиля, производящаяся блоком управления автомобилем. Головным устройством, расположенным на приборной панели соединено все между собой центральным шлюзом.

(Слайд 4) Ethernet-камеры могут дополнительно использовать «энергоэффективный Ethernet» (IEEE 802.3az), в рамках которого вводится Low-Power Idle (LPI, «режим простоя») и пробуждение по необходимости для экономии энергии, пока камеры не используются. Кроме того, решения для питания через Ethernet (PoE) являются предпочтительнее, поскольку они позволяют уменьшить количество проводов. Преимущества более высокой пропускной способности и низкого времени ожидания очевидны. Использование нескольких камер высокого разрешения для обнаружения объекта требует несжатой передачи данных, чтобы избежать образования артефактов сжатия при обнаружении препятствий, а также сильного драйвера с высокой пропускной способностью.

(Слайд 5) Сеть связи будет иерархически организована с контроллерами домена, подключенными через магистраль Ethernet. Подсети ниже контроллеров домена могут также быть на основе Ethernet, с переключателями между уровнями. Эта структура обеспечивает масштабируемое решение, поскольку каждый порт коммутатора в общем случае может быть реализован как 10-Мбит, 100-Мбит и 1-Гбит без каких-либо изменений в высших уровнях протокола. Новизна подхода заключается в том, каким образом сообщение передается через доменные границы к месту назначения. В современных сетях и межсетевых интерфейсах реализация этой функции заключается в IP-маршрутизации с помощью коммутаторов и роутеров, что и предлагается для магистральных сетей. Преимущество заключается в полной независимости IP-маршрутизации от конкретной реализации, что позволяет создать единое решение для автомобильной сети. Кроме того, идея IP позволяет легко подключить автомобиль к Интернету

(Слайд 6) В качестве основного метода исследования использовали собственно собранный испытательный стенд, состоящий из устройства Vector VC121-12 ECU, предназначенного для прототипирования и мелкосерийного производства спортивных автомобилей и сельскохозяйственных машин. Оснащен интерфейсом Flex Ray, 6 CAN, 2 LIN и 1 Ethernet Broad-Reach. Более подробную информацию об этом можно найти в техническом описании; устройства Vector VN5 610A – для связи сетевого интерфейса в ПК.

Этот ECU использует физический уровень 100Base-T1. Для связи с персональным компьютером (ПК) необходим сетевой интерфейс для взаимодействия между двумя различными физическими уровнями 100Base-T1 блока ECU и 100Base-TX.

Зеленая линия на рисунке представляет автомобильное Ethernet-соединение от ECU, а синяя линия представляет стандартный Ethernet-порт 100Base, который подключается к конвертеру Ethernet-USB через USB-порт. На компьютере установлен виртуальный компьютер Mac с операционной системой Kali Linux. Кали была выбрана по нескольким причинам. Во-

первых: OS специально разработан для тестирования на проникновение, отсюда и множество необходимых инструментов. Вследствие строгой регламентации корпоративных программ, утвержденных отделом обработки данных, они могут быть установлены в Windows. В виртуальной машине, с другой стороны, единственное правило заключается в том, чтобы хранить его и отключать доступ к файлам компании.

(Слайд 7) Пакеты программ отправлялись туда и обратно между виртуальной машиной и ECU. Запросы по разным протоколам отправлялись в ЭБУ. Измеряли время отклика и скорость передачи пакета данных. Протестированными протоколами являются ICMP (эхо-запросы), TCP (инициализация соединения TCP с отправкой пакета с установленным флагом SYN) и UDP (используется в сообщениях запроса идентификации транспортного средства DoIP). Все пакеты отправлялись сто раз, а минимальное, среднее и максимальное время ответа сохранено. Минимальное, среднее и максимальное время отклика приведены в таблице.

Для сетевого протокола ICMP были отправлены эхо-запросы и собраны соответствующие эхо-ответы. Время между моментом отправки запроса и моментом получения соответствующего ответа измеряется как время ответа.

(Слайд 8) Рисунок показывает, как выглядит нормальный процесс прошивки с vFlash. В дальнейшем можно увидеть захват Wireshark связи TCP между vFlash и ECU. Показывает, что происходит, если tcp kill запускается до запуска процесса перепрошивки. Появляется сообщение об ошибке «Связь не удалась» и RST помечает TCP

(Слайд 9) Как только скрипт запускается, линии на графике становятся неправильными, как показано на рисунке. Это доказывает, что подделка возможна. В данном примере последствия представляют собой просто некорректный график. Однако то же самое можно было бы сделать с потоком с камеры, который подается в систему управления оперативным движением, которая отвечает за поддержание заданного расстояния от автомобиля впереди. Последствия такой атаки пугающие. SOME / IP все еще является относительно новым протоколом, над которым ведется работа.

Рассматриваются некоторые опции безопасности, такие как Secure Onboard Communication (SecOP) и d(TLS). Другим решением было бы использование безопасного протокола передачи данных в реальном времени, который обеспечивает шифрование, целостность и аутентификацию сообщений в сочетании с мультимедийным интернет-ключом, который ключевое решение для управления, которое предоставляет сеансовые ключи для SR TP.

(Слайд 10) Контрмеры пористости и ограничения перечислены в Таблице. Все контрмеры можно сгруппировать по следующим трем категориям:

1. Использование существующих параметров конфигурации
2. Дальнейшее развитие реализации стека и добавление функций, таких как шифрование и подписи с кэшами, для всех коммуникаций.
3. Изменение существующей реализации стека, чтобы она не соответствовала спецификациям протокола для большей пользы. Примером здесь является отправка помеченных RST TCP-пакетов, когда помеченные SYN-пакеты принимаются на закрытых TCP-портах. Это не будет иметь больших последствий для функциональности системы, но устранил одно воздействие.

Обобщая вышесказанное можно сделать вывод, что фактическая безопасность может быть увеличена на 1,5 RAV, просто изменив конфигурации существующей реализации стека без дальнейшей разработки. Есть две вещи, которые нужно иметь в виду: Во-первых, оценки RAV кажутся низкими из-за того факта, что некоторые контроли вообще не исследовались, поскольку они не имеют отношения к данному исследованию. Во-вторых, некоторые меры безопасности, такие как шифрование, потребуют дополнительных ресурсов и могут снизить производительность системы. Следовательно, существует компромисс между безопасностью и производительностью, который должен оцениваться в каждом конкретном случае в данном сценарии.

(Слайд 11) Таким образом, цель работы достигнута. Спасибо за внимание! Доклад окончен.