УДК **629.3.064.5 + 004.056** Вестник УрФО № 1(27) / 2018, с. 29–33

Синьков А. С., Лужнов В. С.

АНАЛИЗ БЕЗОПАСНОСТИ CAN-ШИНЫ ТРАНСПОРТНЫХ СРЕДСТВ

Безопасность представляет собой фундаментальную проблему в современных транспортных средствах. В них добавляются множество систем, включающих электронные блоки управления, которые связаны между собой системной шиной – Controller Area Network (CAN), являющейся самой важной частью автомобиля. Она основана на протоколе CAN, который не обеспечивает должной безопасности, что показано в данной статье. В статье содержится описание самого протокола и основных принципов его функционирования. Также рассмотрены возможные сценарии атак, которые позволяют злонамеренным злоумышленникам препятствовать системам управления автомобилем и наносить вред автомобилю даже пассажирам, их виды и устройства, с помощью которых их возможно осуществить. Выделены меры защиты транспортных средств от взлома CAN-шины.

Ключевые слова*: Информационная безопасность, CAN-шина, безопасность автомобильных систем, Controller Area Network, безопасность транспортных средств.*

Sinkov A. S., Luzhnov V. S.

SECURITY ANALYSIS OF CAN-BUS VEHICLES

Safety is a fundamental problem in modern vehicles. In cars, many systems are added, including electronic control units, which are connected by a system bus – the Controller Area Network (CAN), which is the most important part of the car. It is based on the CAN protocol, which does not provide the necessary security, as shown in this article. The article contains a description of the protocol itself and the basic principles of its functioning. Also considered are possible attack scenarios that allow malicious cybercriminals to interfere with vehicle control systems and damage the car even to passengers, their types and devices by which they can be carried out. Measures to protect vehicles from hacking CAN bus.

Keywords*: Information security, CAN-bus, safety of automobile systems, Controller Area Network, safety of vehicles.*

Увеличение сложности технологий, внедряемых в современные автомобили растёт с каждым годом, что увеличивает их функциональность, но одновременно с этим и несет все больше уязвимостей в безопасности. Злоумышленники могут злоупотреблять найденными уязвимостями и наносить вред самому автомобилю, а также пассажирам.

В современных транспортных средствах устанавливается ряд электронных блоков управления (ЭБУ), которые управляют различными функциями автомобиля. Все они

связаны между собой системной шиной контроллера (CAN – Controller Area Network). Она имеет протокол для последовательной связи, обеспечивает достаточно высокий уровень безопасности и поддерживает распределенное управление электронными блоками управления (ECU) в реальном времени [1]. При этом протокол CAN не обеспечивает конфиденциальности и аутентификации для кадров, пересылаемых по шине. CAN-шина передает информацию кадрами, которые транслируются сразу во всю сеть, что сразу же вызывает много проблем безопасности, таких как перехват.

Преимущества при использовании CAN протокола:

– обеспечивает большую скорость передачи (до 1 Мбит/с);

– протокол CAN успешно реализован в системах реального времени;

– обеспечивает хорошее соотношение производительности и цены;

– информация передается сразу всем узлам сети короткими кадрами;

– надежный контроль за ошибками передачи и приема;

– высокая устойчивость к помехам.

Существует 4 типа CAN-сообщений:

– кадр данных (Data Frame) – стандартное сообщение;

– кадр запроса передачи (Remote Frame) – это Data Frame, но без поля с данными, чаще всего необходимы для запроса передачи данных;

– кадр ошибки (Error Frame) – передается узлом при нарушении формата принятого сообщения;

– кадр перегрузки (Overload Frame) – используется перегруженным узлом для просьбы повтора сообщения.

Распространены несколько версий протокола: CAN 2.0A и CAN 2.0B, последний также именуется, как Extended CAN. Они отличаются размерами кадров и скоростями передачи. В таблице представлены кадры для стандартной версии протокола (2.0A) и расширенной (2.0B) [1]. В стандарте 2.0B скорость передачи варьируется в диапазоне от 125 Кбит/с до 1 Мбит/с, ее определяет, в большей степени, дина кабеля. Максимальная скорость обеспечивается в сети до 40 метров [1]. В тоже время в стандарте 2.0A максимальная скорость: 125 Кбит/с.

Кадр данных для 2.0A и 2.0B

Поле	Длина (бит) для 2.0A	Длина (бит) для 2.0B	Описание
Начало кадра (SOF)	1	1	Указывается доминантный бит
Базовый идентификатор	11	11	Уникальный идентификатор, определяющий приоритет
Бит подмены запроса на передачу (SRR)	Поле отсутствует	1	Рецессивный бит
Поле расширения идентификатора	Поле отсутствует	18	Расширение поля арбитража для расширенного формата
Удаленный запрос передачи (RTR)	1	2	Доминантный бит в поле данных для 2.0A и рецессивные биты для 2.0B (для Remote Frame – индикатор получения)
Зарезервированное	2	Поле отсутствует	Доминантные биты
Код длины данных (DLC)	4	4	Число байт в поле данных (0-8)
Поле данных	0-8 байт	0-8 байт	Длина определяется полем DLC
Поле циклического контроля избыточности (CRC)	15	15	Контрольная последовательность, формируемая БЧХ-кодом (до 127 бит)
Разделитель CRC	1	1	Должен быть рецессивным битом
Поле подтверждение приема (ACK)	1	1	Отправитель записывает рецессивный бит, получатель – доминантный бит
Разделитель ACK	1	1	Должен быть рецессивным битом
Конец кадра (EOF)	7	7	Состоит из рецессивных битов
Итого без поля данных, бит:	45	62	

Стоит отметить, что, используемые в таблице термины рецессивный и доминантный, описывают двоичные состояния «0» и «1» соответственно.

Порядок передачи битов в кадре данных для версий протокола 2.0A и 2.0B представлены на рис. 1.

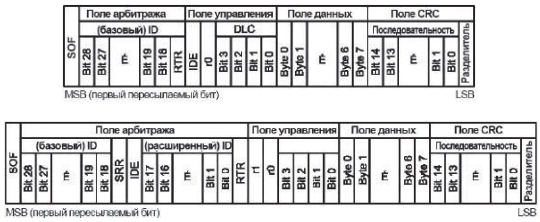

Рис. 1. Порядок передачи битов (сверху – базовый формат 2.0A, снизу – расширенный 2.0B)

При получении доступа к CAN-шине (например, через диагностический разъем ODB-II [2]), злоумышленник может совершать различные действия с автомобилем, вплоть до полной его остановки, что может привести к катастрофическим последствиям.

ЭБУ соединены друг с другом на нескольких шинах, соответствующих спецификациям CAN. Связь осуществляется между ЭБУ путем отправки CAN-пакетов. Компоненты не могут определить откуда прибыл пакет CAN, поскольку протокол не поддерживают какую-либо форму аутентификации, поэтому легко для любого пакетного сниффера перехватывать исходный пакет, маскировать как законный пакет или отправлять ложные данные в CAN-пакеты. Из-за отсутствия аутентификации, обратная трассировка скомпрометированного ЭБУ, который отправляет вредоносные атакующие пакеты на CAN, практически невозможна в режиме реального времени [3]. В связи с этим возникает возможность, отслеживая сеть CAN и ЭБУ, генерировать ложные сообщения, чтобы ЭБУ инициировал выполнение определенного действия.

Подключится к CAN-шине автомобиля для получения сообщений можно, например, с помощью двуканального осциллографа. Необходимо найти витую пару, принадлежащая CAN-шине и снимать с них сигнал. Однако наиболее простой способ подключение к CAN-шине автомобиля – через порт OBD-II. Данный разъем устанавливается во все современные транспортные средства. Основная его цель – диагностика обслуживания двигателя и транспортных средств. Наиболее популярные устройства, подключаемые к данном порту: ELM327, CARDAQ-Plus, Launch CReader и др. Также существует устройство CANCrocodile (рис. 2), которое подключится к витой паре автомобиля без нарушения оплетки проводов, т. е. считывание происходит без физического контакта с проводами [4]. Оно изначально предназначалось для подключения к шине CAN систем GPS/ГЛОНАСС мониторинга, однако возможно и подключение, например, к компьютеру посредствам дополнительного устройства MasterCAN Tool, который считывает и анализирует данные с шины.

Рис. 2. Устройства для подключения к CAN-шине (слева направо: CANCrocodile, ELM327, Launch CReader)

Для отправки пакетов через CAN-шину можно воспользоваться готовым адаптером, например, ELM327, либо собрать собственный адаптер, например, из Arduino Uno, микрочипа MCP2551 и разъема SAE J1962 [5].

Возможные сценарии атаки

Узлы в сети CAN могут использовать энергозависимую (RAM) и (или) энергонезависимую (flash) память. Любой узел может быть, как отправителем сообщений, так и получателем.

Как уже упоминалось, CAN-шина не имеет никакой аутентификации. Поэтому, если злоумышленнику удастся получить доступ к шине, он может получить код, запущенный на ЭБУ. Кроме того, он может полностью управлять автомобилем, отправляя поддельные сообщения. В связи с этим, возможны несколько сценариев получения доступа к CAN-шине транспортного средства с целью отправки сообщений:

– Сценарий 1: злоумышленник использует дополнительное внешнее устройство для доступа к шине, присоединив его, например, к диагностическому порту OBD-II.

– Сценарий 2: злоумышленник получил доступ к сети CAN, скомпрометировав один из существующих ЭБУ автомобиля.

– Сценарий 3: если автомобиль оснащен доступом в сеть Интернет, то злоумышленник, обойдя штатную систему защиты, может получить доступ к шине.

Последний сценарий атак наиболее привлекателен для злоумышленников, поскольку нет необходимости непосредственной модификации систем автомобиля, будь то компрометация ЭБУ или установка OBD-II устройства, а также в связи с возрастанием интегрированности сети Интернет, необходимого для удаленного диагностики, тематики. В частности, транспортные средства марки Tesls используют Интернет-соединение для обновления внутренних систем автомобиля [6].

После получения доступа к CAN-шине автомобиля, злоумышленник может либо отправлять поддельные сообщения, либо повторно посылать прослушанные сообщения [7].

При атаке с отправкой фальшивых сообщений, противник пытается отправить поддельное сообщение, заявив себя в качестве другого ЭБУ, то есть используя отличный идентификатор узла от назначенного ему в сообщении аутентификации.

Возможно, также, полностью отключить какой-то узел от шины путем отправки большого количества ошибочных кадров, связанных с определенным узлом, после чего узел отключается от общей шины [5]. Таким образом можно отключить важные системы автомобиля, путем штатного механизма обработки ошибок протокола CAN, не позволяющей влиять отказавшим узлам на работу всей системы.

Для второго вида атак (дублирование сообщений) первоначально злоумышленнику необходимо некоторое время считывать сообщения, пересылаемые, между блоками и выделить среди них необходимые. Поскольку протокол CAN не поддерживает аутентификацию сообщения, ЭБУ-получатель не может идентифицировать данные в сообщении и выполняет функцию, которая находится в пакете CAN. Например, если злоумышленник хочет атаковать тормоза транспортного средства, он должен непрерывно отправлять пакет, вызывающий блокировку тормозных дисков.

В качестве примера, рассмотрим автомобиль Ford Escape [7]. Чтобы остановить двигатель, а точнее, блокировать цилиндры, достаточно непрерывно отправлять пакеты вида: IDH: 30, IDL: F5, Len: 08, Data: FF FF FF FF FF FF FF FF. Также имеется возможность изменить показания спидометра, посылая ложные пакеты по CAN-шине. Возможно отключение всех осветительных приборов в автомобиле (для выключения требуется, чтобы он не был в движении) и даже тормозной системы, путем отправки команды 0x003C [3].

Способы защиты

Наиболее кардинальный и действенный способ защиты – это отключение всех систем, использующих Интернет-соединение и ограничение круга лиц, которые имеют доступ к автомобилю, и слежение за действиями людей, допущенных к нему, для избегания установки дополнительных устройств, подключаемых к CAN-шине.

В настоящее время широко применяют шифрование данных. Так, для защиты системы достаточно шифровать отправляемые сообщения каждым ЭБУ, однако при таком подходе теряется скорость обмена сообщениями.

Для защиты от 3 сценария атак разрабатываются блоки управления шлюзом связи, который защищает внутренние системы автомобиля от внешней среды. Так, компании Kaspersky и AVL создали прототип такого устройства – модуль безопасного соединения (Secure Communication Unit – SCU) [8]. Данное устройство позволяет обмениваться блокам внутри автомобильной сети в обход SCU, что положительно сказывается на скорости работы.

Литература

1. ГОСТ Р ИСО 11898-1-2015. Транспорт дорожный. Местная контроллерная сеть (CAN). Часть 1. Канальный уровень и передача сигналов.

2. Carsten P., Andel T.R., Yampolskiy M., McDonald JT. In-vehicle networks: attacks, vulnerabilities, and proposed solutions. In: Proceedings of the 10th annual cy- ber and information security research conference. ACM; 2015. p. 1.

3. Miller C., Valasek C. Adventures in automotive networks and control units. Def Con 2013; Volume 21, p.260–264.

4 CANCrocodile безопасное получение данных CAN шины // Технотон. URL: http://www.technoton.by/crocodile/cancrocodile (дата обращения 10.12.2017).

5. Palanca A., Evenchick E., Maggi F., Zanero S. A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks // Springer International Publishing. 2017. Vol. 10327. P. 185-206. doi: 10.1007/978-3-319-60876-1

6. Software updates // Tesla. URL:https://www.tesla.com/support/software-updates (дата обращения 25.12.2017).

7. Wang Q., Sawhney S. Vecure: a practical security framework to protect the can bus of vehicles. In: Internet of Things (IOT), 2014 international conference on the. IEEE; 2014. p. 13–18.

8. Умный автомобиль – безопасный автомобиль: «Лаборатория Касперского» и AVL представили модуль для киберзащиты для современных машин // Kaspersky lab. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-and-avl-presented-module-for-cyber-defense-for-modern-machines (дата обращения 22.12.2017)

References

1. GOST R ISO 11898-1-2015. Transport dorozhnyj. Mestnaja kon-trollernaja set' (CAN). Chast' 1. Kanal'nyj uroven' i peredacha signalov.

2. Carsten P., Andel T.R., Yampolskiy M., McDonald JT. In-vehicle net-works: attacks, vulnerabilities, and proposed solutions. In: Proceedings of the 10th annual cy- ber and information security research conference. ACM; 2015. p. 1.

3. Miller C., Valasek C. Adventures in automotive networks and control units. Def Con 2013; Volume 21, p.260–264.

4 CANCrocodile bezopasnoe poluchenie dannyh CAN shiny // Tehnoton. URL: http://www.technoton.by/crocodile/cancrocodile (data obrashhenija 10.12.2017).

5. Palanca A., Evenchick E., Maggi F., Zanero S. A Stealth, Selective, Link-Layer Denial-of-Service Attack Against Automotive Networks // Springer Inter-national Publishing. 2017. Vol. 10327. P. 185-206. doi: 10.1007/978-3-319-60876-1

6. Software updates // Tesla. URL:https://www.tesla.com/support/software-updates (data obrashhenija 25.12.2017).

7. Wang Q., Sawhney S. Vecure: a practical security framework to protect the can bus of vehicles. In: Internet of Things (IOT), 2014 international confer-ence on the. IEEE; 2014. p. 13–18.

8. Umnyj avtomobil' – bezopasnyj avtomobil': «Laboratorija Kas-perskogo» i AVL predstavili modul' dlja kiberzashhity dlja sovremennyh mashin // Kaspersky lab. URL: https://www.kaspersky.ru/about/press-releases/2017_kaspersky-lab-and-avl-presented-module-for-cyber-defense-for-modern-machines (data obrashhenija 22.12.2017)

СИНЬКОВ Антон Сергеевич, студент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: sinkov_96@mail.ru

ЛУЖНОВ Василий Сергеевич, ассистент кафедры защиты информации высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: ua9stz@gmail.com

SINKOV Anton, student of the department of information security of the school of electrical engineering and computer science «South Ural State University (national research university)». 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: sinkov_96@mail.ru

LUZHNOV Vasiliy, Assistant of the Information Security Department of the Higher School of Electronics and Computer Science "South Ural State University (National Research University)". 76, Lenin prospect, Chelyabinsk, Russia, 454080. E-mail: ua9stz@gmail.com