Анализ безопасности CAN-шины автомобилей

С.Б. Калинин [1], А.О. Гасников [1], И.С. Теннант [1]

[1]Санкт-Петербругский государственный электротехнический университет «ЛЭТИ»,
Россия, 197022, г. Санкт-Петербург

Аннотация. В данной статье рассматриваются основные уязвимости CAN-протокола автомобильных систем, в том числе возможность несанкционированного воздействия на ключевые узлы транспортного средства. Особое внимание в рамках исследования уделялось рассмотрению возможных уязвимостей OBD порта, через который можно получить несанкционированный доступ к CAN-шине, а также аналогичные возможности проведения атак через беспроводные интерфейсы (Bluetooth, Wi-Fi, LTE). Для подтверждения возможности инициирования атак удаленного доступа была проанализирована связь между беспроводными интерфейсами и CAN-шиной. Результаты показывают, что при наличии уязвимостей в шлюзах и конфигурациях возможно управление критическими функциями автомобиля через удалённый доступ.

Ключевые слова: CAN-протокол, OBD порт, беспроводные интерфейсы, удаленное управление, информационная безопасность.

Abstract. This article examines the main vulnerabilities of the CAN protocol in automotive systems, including the potential for unauthorized access to critical vehicle components. Special attention was given to exploring vulnerabilities in the OBD port, which can provide unauthorized access to the CAN bus, as well as similar attack vectors via wireless interfaces (Bluetooth, Wi-Fi, LTE). To confirm the feasibility of remote access attacks, the connection between wireless interfaces and the CAN bus was analyzed. The findings indicate that if vulnerabilities exist in gateways and configurations, critical vehicle functions can be controlled remotely.

Keywords: CAN-bus, OBD port, wireless interfaces, remote control, information security.

Введение

Протокол Controller Area Network (CAN) широко применяется для организации сетей встраиваемых систем и нашел своё применение в автомобильной промышленности, аэрокосмической отрасли, сельском хозяйстве, медицинских устройствах, а также в некоторых бытовых и коммерческих приборах. В автомобильных системах CAN-шина обеспечивает передачу данных между электронными блоками управления (ECU), что делает её неотъемлемой частью современных транспортных средств. Однако, несмотря на все преимущества, использование CAN-шины сопряжено с рядом уязвимостей, связанных с архитектурными особенностями протокола и недостатками в его реализации.

С начала 2017-х годов было выявлено множество уязвимостей CAN-шины, обусловленных отсутствием аутентификации и шифрования, а также недостаточной сегментацией сети, что позволяет злоумышленникам внедрять несанкционированные устройства, взаимодействующие с ECU, и осуществлять атаки, такие как DoS (Denial of Service) путем отправки доминантных битов с высоким приоритетом. В данной работе рассматриваются основные способы несанкционированного воздействия на CAN-шину автомобиля, включая доступ через диагностический порт (OBD), использование беспроводных интерфейсов и уязвимости, связанные с взаимодействием рассматриваемых технологий.

1. Несанкционированный доступ через OBD порт

CAN-шина реализована как пара дифференциально сбалансированных сигнальных проводов (CAN_H и CAN_L), что обеспечивает высокую помехоустойчивость и отказоустойчивость системы, снижая электромагнитные помехи. Биты, передаваемые по шине, могут быть доминантными (логический ноль) или рецессивными (логическая единица), причём доминантные биты имеют больший приоритет при передаче сообщений. OBD порт используется для диагностики автомобиля, позволяя считывать данные с датчиков и изменять параметры работы двигателя. (рисунок 1).

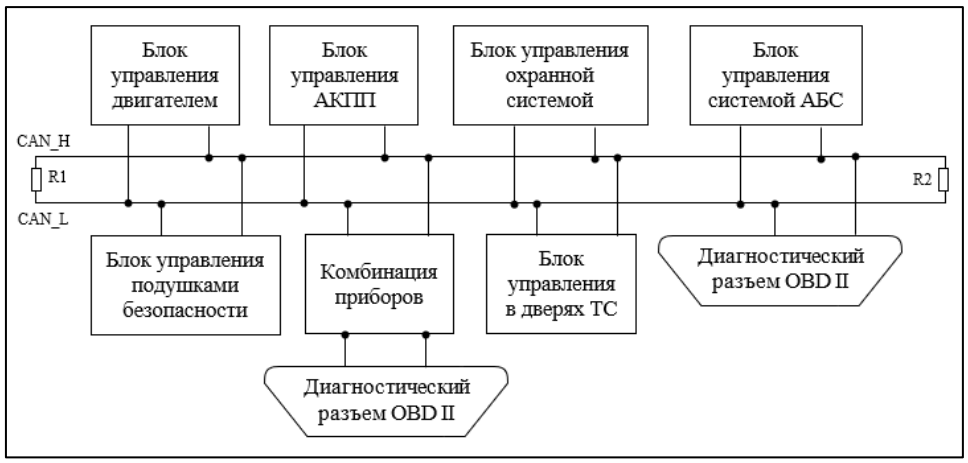

Рисунок 1 – Типовая схема шины CAN

В исследовании Роберта Буттиджича [1], посвящённому проблемам безопасности в сетях контроллеров автомобилей, было продемонстрировано, как злоумышленники смогли использовать стандартные диагностические команды для перепрограммирования ECU (Electronic Control Unit). В экспериментах с подключением к OBD-II исследователи смогли

внедрить фальшивые сообщения в критически важные ECU, что привело к сбоям в работе тормозов, глушению двигателя, отображению поддельных значений на комбинации приборов, и даже отключению систем внутреннего и внешнего освещения. В некоторых случаях также возможно использование платы Arduino, подключённой к OBD-II, для создания удалённого доступа через Bluetooth.

Многие современные автомобили оборудованы шлюзами (Gateway), которые ограничивают доступ к другим частям сети через OBD-II. Однако наличие данного подхода не исключает возможность проведения рассматриваемых атак, поскольку злоумышленник может выполнить диагностику и атаковать непосредственно те сегменты сети, которые остаются доступными.

Таким образом, при подключении через OBD атакующий может:

- изменять режим работы двигателя;
- активировать или деактивировать системы безопасности (например, подушки безопасности);
- воздействовать на тормозную систему;
- управлять стеклоподъёмниками или рулевым управлением.

В работе [2] авторы также рассматривали атаку на OBD порт, которая была осуществлена посредством физического доступа нему, благодаря чему удалось внедрить поддельные пакеты в CAN-шину, из-за чего работа тормозной системы была скомпрометирована. Злоумышленник может обладать знаниями о том, какие CAN-сообщения назначены критически важным функциям транспортного средства, которые он может почерпнуть из реверсивного подхода или из общедоступной базы данных (например, OpenDBC), что упрощает построение вектора атаки. Таким образом, можно сделать вывод, что CAN-шина крайне уязвима к инъекционным атакам, проходящим через OBD порт.

2. Подключение через беспроводные интерфейсы

Растущая потребность в подключении транспортных средств к внешним сервисам привела к интеграции технологий, таких как Wi-Fi, Bluetooth, 3G/4G и GPS. Данные технологии расширяют функциональность автомобилей, но также создают дополнительные векторы атак. Рассматривая средства беспроводной коммуникации (в том числе повсеместно использующиеся в автономных электромобилях), важно упомянуть уязвимость к спуфингу, удалённому управлению программной системы и беспроводных протоколов коммуникации, неавторизованному доступу к критически важным структурам автомобиля и другие методы для компрометации системы.

Например, атака через Bluetooth может быть реализована двумя способами:

1) Непрямая атака: Установка вредоносного ПО на устройство владельца автомобиля. При подключении к телематической системе автомобиля программа активирует триггер, который позволяет злоумышленнику получить контроль над ECU;
2) Прямая атака: обнаружить и идентифицировать MAC-адрес автомобиля и установить с ним сопряжение (Bluetooth). Так как подобный процесс, как правило, протекает незаметно для владельца, то ничего не мешает инициировать процесс подбора сгенерированного пароля для подтверждения сопряжения.

Данные атаки особенно опасны, поскольку позволяют злоумышленнику получать доступ к критически важным функциям автомобиля.

В исследовании Знити Асмае [3] приведено решение, эксплуатирующее уязвимость CAN-шины к удалённому внедрению вредоносных сообщений и нарушению нормальной работы сети. Атака производилась на узле, использующем протокол связи Bluetooth. Благодаря постоянной отправке с сопряженного вредоносного мобильного устройства злоумышленника ложного значения температуры на CAN-шину с идентификатором с высоким приоритетом, удалось привести систему в состояние, при котором другие узлы вынуждены прекратить свои трансляции и исказить реальное значение температуры, а также ввести пользователя в заблуждение о наличии проблемы. При этом использовалось программное обеспечение на операционной системе Android для генерации шестнадцатеричного файла и его загрузку на различные карты Arduino через Bluetooth. В тот момент, когда Arduino получает данные на свой порт, он автоматически проверяет, что полученная последовательность символов указывает на то, что есть новая программа, которую нужно загрузить.

В исследовании Дамилолы Оладимеджи, [2] также содержится упоминание атаки, проведённой удалённо через уязвимые узлы, такие как CD-плееры, Bluetooth и радиоприёмники, благодаря которым дверь автомобиля может быть разблокирована с помощью удалённого доступа. При этом также обозначена возможность проведения атаки через Wi-Fi [4], в которой злоумышленники могут получить доступ к системам торможения и рулевого управления. Более сложные сценарии атак включают использование нескольких векторов воздействия — от подмены пакетов данных до внедрения вредоносного ПО на уровне ECU.

3. Взаимодействие между беспроводными интерфейсами и CAN шиной

Для оценки рисков управления узлами автомобиля через беспроводные интерфейсы важно понять, существует ли физическая или программная связь между ними и CAN-шиной. Первоначально CAN был изобретен как единая последовательная шина, соединяющая все узлы в рамках единой сети. Поскольку все сообщения транслируются по широковещательному типу сети, любой ECU [5] может отправлять сообщения на другие критически важные ECU, такие как блок управления торможением. Каждый узел построен с механизмом фильтрации сообщений, который разделяет сообщения на основе их идентификаторов и рассматривает только те, которые имеют к нему непосредственное отношение, игнорируя остальные. Кроме того, узлы в сети могут быть легко добавлены или удалены, поскольку не требуется никаких изменений в аппаратном и программном обеспечении или на прикладном уровне. Рассматриваемая уязвимость облегчает неавторизованным устройствам связь с другими ECU, которые отвечают за безопасность автомобиля. Кроме того, если злоумышленник получит доступ к кабелям CAN, он сможет получить доступ ко всей сети и управлять критически важными ECU, такими как тормоза, двигатель или системы освещения.

Исследования показали, что многие беспроводные интерфейсы имеют прямую или косвенную связь с CAN через шлюзы, что создаёт потенциальную возможность управления автомобилем через удалённый доступ.

Большинство современных автомобилей используют шлюзы для разграничения внутренних (CAN) и внешних (беспроводных) сетей. Такие шлюзы выступают в роли фильтров, предотвращая несанкционированное вмешательство. Однако ошибки в

программной реализации или недочёты в конфигурации могут открывать доступ к внутренней сети. Примером эксплуатации подобных уязвимостей является ранее рассмотренная атака через Bluetooth-соединение, при которой уязвимость в шлюзе позволила перехватить и перенаправить команды в CAN-шину.

Заключение

В статье рассмотрены основные угрозы и уязвимости, связанные с несанкционированным доступом к CAN-шине автомобилей, а также проанализированы возможности атак через OBD-порт, беспроводные интерфейсы и взаимодействие между ними и CAN-шиной. Результаты показывают, что несмотря на использование шлюзов для изоляции внутренних сетей автомобиля, остаются значительные риски для проведения атак, эксплуатирующих уязвимости рассмотренных элементов. Уязвимости в конфигурации шлюзов и их программной реализации также могут быть использованы для удаленного управления критически важными функциями автомобиля.

Хотя в литературе нечасто приводятся конкретные механизмы эксплуатации найденных уязвимостей, экспериментальные значения, рассмотренные в данной статье, позволяют сделать вывод о возможности вывода злоумышленниками из строя систем тормоза, двигателя, комбинации приборов и прочих благодаря реализации физических или удаленных атак на CAN-шину и связанные с ней элементы, в том числе и ECU, отвечающие за нормальное функционирование систем автомобиля.

Для минимизации угроз предлагается применять многоуровневую защиту, которая бы включала более сложные механизмы аутентификации и шифрование данных, а также сегментацию сети, отсутствие в некоторых моделях автомобилей которой дает возможность реализовывать рассмотренные атаки. Результаты подчеркивают важность создания более безопасной архитектуры для сетей автомобилей, учитывающей современные вызовы кибербезопасности.

Благодарности

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации № 075-00003-24-01 от 08.02.2024 (проект FSEE-2024-0003).

Список литературы

1. Security Issues in Controller Area Networks in Automobiles / R. Buttigieg, M. Farrugia, C. Meli. // 18th international conference on Sciences and Techniques of Automatic control & computer engineering – STA'2017, Monastir, Tunisia. URL: https://doi.org/10.48550/arXiv.1711.05824;
2. CANAttack: Assessing Vulnerabilities within Controller Area Network / D. Oladimeji, A. Rasheed, C. Varol, M. Baza, H. Alshahrani, A. Baz // Sensors. 2023; 23(19):8223. URL: https://doi.org/10.3390/s23198223;
3. Implementation of a bluetooth attack on controller area network (CAN) / Z. Asmae, El Nabih // Indonesian Journal of Electrical Engineering and Computer Science. Vol. 21. pp. 321-327. URL: https://doi.org/10.11591/ijeecs.v21.i1.pp321-327;

4. Real-Time Attack Detection in Modern Automobile Controller Area Networks / E. Martin, S. Shenoi // IFIP Advances in Information and Communication Technology (IFIPAICT), Vol. 686. No 17. pp. 221–252. URL: https://doi.org/10.1007/978-3-031-49585-4_11;
5. Intrusion Detection System CAN-Bus In-Vehicle Networks Based on the Statistical Characteristics of Attacks / Junaid Ahmad, Dae-Woon Lim, Young-Sik Kim // Sensors 23(7):3554. URL: https://doi.org/10.3390/s23073554;
6. Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection / M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, S. J. Prowell // CISRC '17: Proceedings of the 12th Annual Conference on Cyber and Information Security Research. No. 11, pp. 1–4. URL: https://doi.org/10.1145/3064814.3064816.