

Научное саммари

Автомобили Януса: сущностно-ориентированная модель угроз для автомобилей, соответствующих протоколам, при предположении о злонамеренном производителе

Оригинальное название: Janus Vehicles: Entity-Centric Threat Modelling of Protocol-Conformant Vehicles under a Malicious-Manufacturer Assumption

Авторы: Jaeung Franciskus Yoo, Huy Kang Kim

Дата публикации: 2026-10-27

Источник: arXiv

Основа анализа: полный текст открытой версии статьи

Направления: Системы и средства защиты информации

Первоисточник: <https://arxiv.org/abs/2610.37059v1>

1 Резюме

Концептуальная статья о модели угроз для автомобилей, которые остаются аутентичными и протоколно-конформными, но содержат скрытую функциональность, нарушающую заявленное назначение («изначально созданный для злонамеренных действий»). Авторы предлагают сущностно-ориентированный Threat Model из трёх компонентов: архетипы злонамеренных сущностей, матрица «поведение-уровень воздействия» и модель поведенческого взаимодействия. Текст обрывается в начале раздела III, поэтому анализ ограничен видимыми частями: введением, обзором текущей практики и частью классификации типов угроз (Type II и Type III полностью, Type I частично).

2 Проблема и контекст

Автомобильная кибербезопасность в основном исходит из допущения о добросовестном производителе и конструкторском органе и фокусируется на атаках извне, компрометации и узлах сети, проявляющих себя через неправильное поведение. Предполагается, что доставленный автомобиль выполняет заявленную функцию. Протоколно-конформное транспортное средство со скрытой функциональностью (зондирование, внеполосная передача данных, спящее или контекстно активируемое воздействие) может не давать никаких свидетельств, которые ищут детекторы. Регуляторные акты (ISO/SAE 21434, UN R155 и R156, NIS2, CRA) и рекомендации по цепочке поставок (NIST SP 800-161, MITRE

System of Trust, Auto-ISAC TRACK) не требуют явной гарантии того, что вся реализованная функциональность заявлена и служит разрешённой цели, когда сам конструкторский орган может быть недоброжелательным. Авторы отмечают, что сертификация может проходить для «саниitized» образца, а скрытая функциональность добавляется позже через обновления или обслуживание.

3 Цель исследования

Сформулировать концептуальную основу для характеристики и поиска доказательств скрытой, нарушающей назначение функциональности в киберфизической сущности, которая сохраняет конформность своим легитимным протокольным интерфейсам. Исследовательский вопрос: как исследователи могут характеризовать такую угрозу и искать для неё доказательства. Авторы явно указывают, что процедуры сбора доказательств и эмпирическая валидация методики расследования выходят за рамки работы.

4 Методы и модели

Работа носит концептуальный характер: анализ литературы, стандартов и регуляторных документов, а также перенос подходов из поведенческого анализа вредоносного ПО (MBC, MAEC, сигнатурные, эвристические и поведенческие методы). Предложены три компонента: (1) типы злонамеренных сущностей, включающие четыре типа злонамеренных сущностей: автомобили, соблюдающие протоколы, но преследующие злонамеренную цель, скомпрометированные автомобили, повторно использованные подлинные компоненты и имитированные автомобили или компоненты; (2) матрица поведения и уровней воздействия, которая классифицирует скрытые, открытые и маскирующие действия по аппаратным, программным и сетевым уровням воздействия; (3) модель поведенческого взаимодействия, описывающая, как скрытые возможности контекстно активируются, реализуются через действия, проявляются в автомобиле и среде и могут быть замечены или скрыты. Подробное формальное описание матрицы и модели в видимой части текста не приведено; в нём есть только их обзорное описание в перечне вкладов.

5 Данные и экспериментальная постановка

В видимой части текста эмпирических данных, экспериментов, наборов данных и количественных оценок нет. Авторы опираются на открытые сообщения о случаях как на иллюстрации: скандал Volkswagen с про-

граммным обеспечением, распознающим регуляторные испытания; дело Mitsubishi с различием между конструктором и брендом (2016); данные о сборе информации о поездках (ВВС); ограничения в отношении китайских роботов, инверторов и автобусов; взрывные пейджеры в Ливане. Авторы подчёркивают, что не все эти случаи однозначно доказывают злонамеренность, часть из них находится на стадии расследования или превентивных ограничений.

6 Результаты

Количественных или экспериментальных результатов в видимой части нет. Основные выводы авторов (концептуальные, а не эмпирические): (1) аутентичность и протокольная конформность не доказывают конформность назначению; (2) поведенческое обнаружение и системы управления доверием реактивны и могут не предотвратить однократную атаку; (3) повторно использованные компоненты могут оставаться подлинными и сохранять идентичности и возможности вне санкционированного контекста, что снижает эффективность сигнатурного снятия отпечатков и аутентификации на основе сертификатов; (4) текущая регуляция и исследования не устанавливают явного требования гарантировать, что вся функциональность заявлена и служит разрешённой цели. Последние два пункта частично опираются на аргументацию авторов и не подтверждены измерениями в тексте.

7 Ограничения

Авторы прямо указывают, что не предлагают модель или процедуру расследования, а также не проводят эмпирическую валидацию. Работа ограничена концептуальным уровнем. В видимом тексте раздел III обрывается, поэтому полная структура модели и определения всех типов угроз проверить нельзя. Часть иллюстративных случаев не подтверждает злонамеренность, на что сами авторы обращают внимание. Практическая применимость матрицы и модели к реальным автомобилям не показана.

8 Воспроизводимость

Воспроизводимость в экспериментальном смысле неприменима: работа концептуальная. Данных, кода, протоколов испытаний и приложений в видимом тексте нет. DOI в метаданных не указан; статья указана как препринт, принятый к публикации на PRDC 2026. Полный текст, включая раздел III и последующие, для окончательной оценки требуется получить.

9 Связь с тематическими направлениями

Работа актуальна для автомобильной кибербезопасности, CPS, регулирования (UN R155/R156, NIS2, CRA), управления рисками цепочки поставок, закупок и одобрение типа транспортного средства, а также для расследований, где поставщик или производитель может сам представлять угрозу. Она связывает подходы поведенческого анализа вредоносного ПО с задачей оценки доверия к конечному изделию, а не только к его компонентам или сетевым узлам.

10 Что не удалось установить

Полнота предложенной модели неизвестна из-за обрыва текста. Степень применимости матрицы и модели на практике не оценена. Не ясно, как именно будут получены и оценены доказательства в условиях, когда сама сущность может скрывать функциональность и уничтожать следы. Иллюстративные кейсы не всегда подтверждают злонамеренность, поэтому их роль как доказательства ограничена. Дата в метаданных (2026) и принадлежность к arXiv указаны в метаданных и не проверялись по внешним источникам.

Ссылки

Первоисточник: <https://arxiv.org/abs/2610.37059v1>

PDF статьи: <https://arxiv.org/pdf/2610.37059v1>