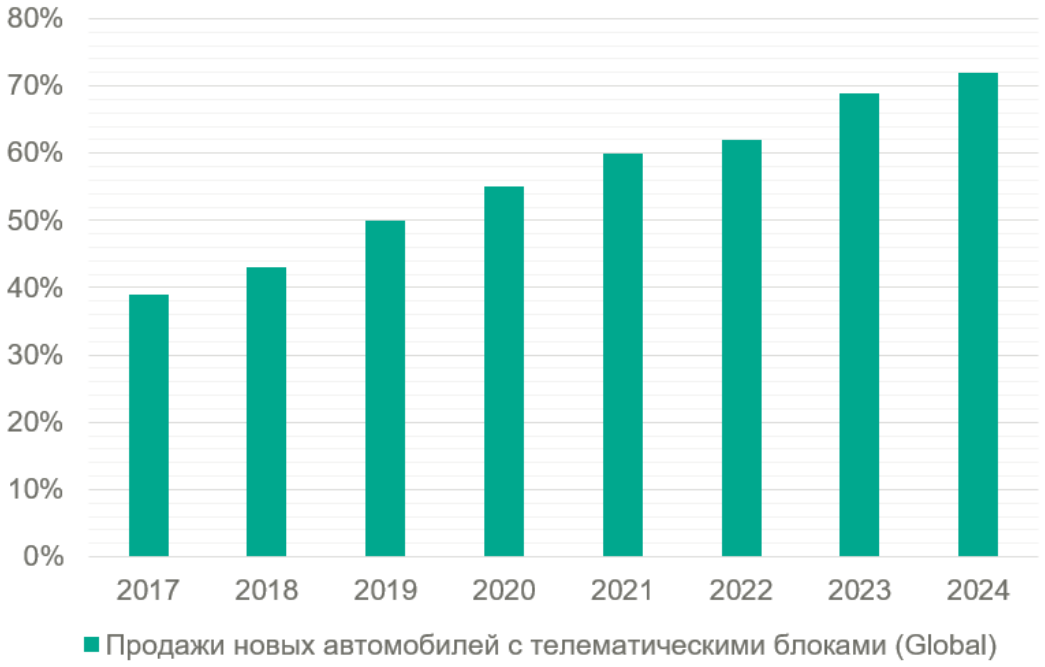
kaspersky

Кибер-иммунитет транспортных систем

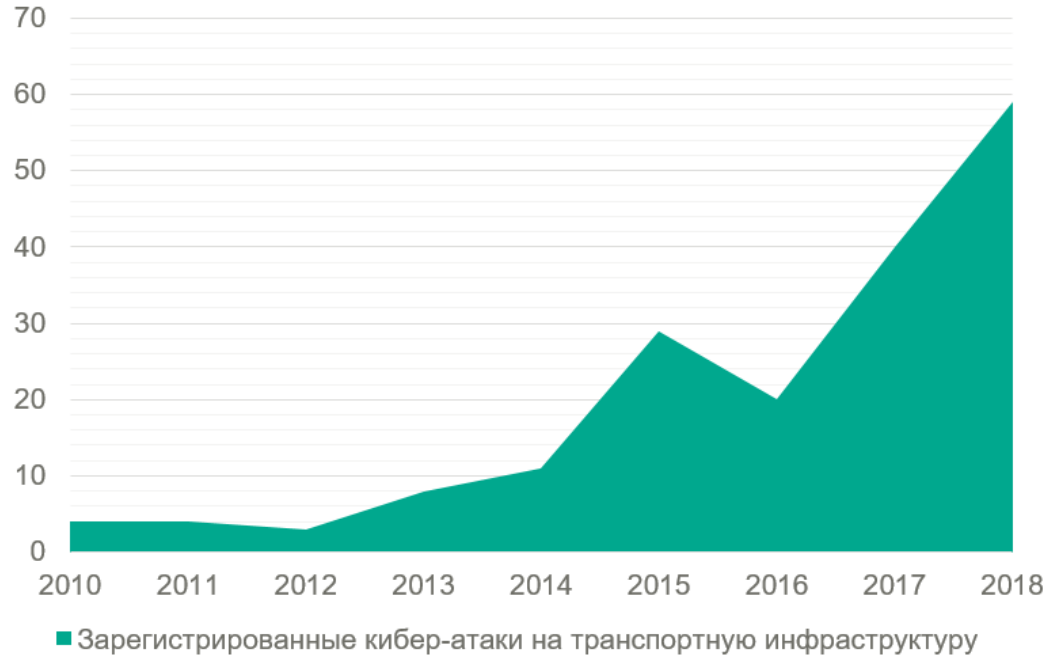
Киберугрозы для ТС стали реальностью

Количество «подключенного» транспорта



IHS Markit report, 2018

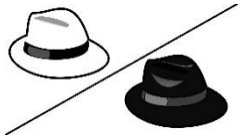
Количество кибератак



Uptane Security, 2019

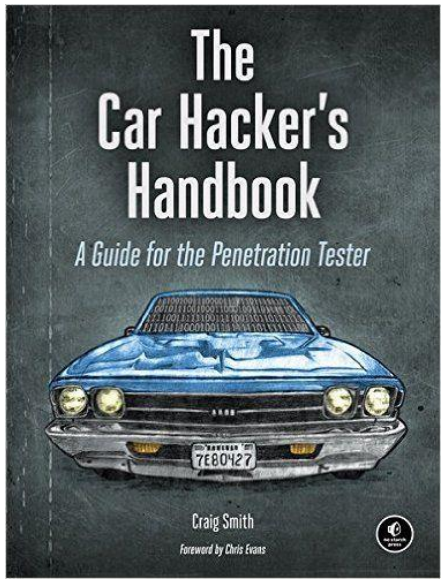
kaspersky

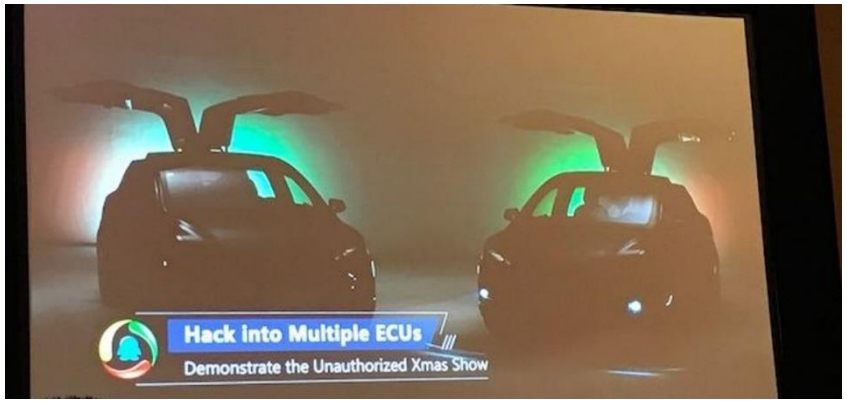
Киберугрозы для ТС стали реальностью



Wi-Fi connectivity for mobile app control v unusual

NOT Wi-Fi for internet access, as per some VAG vehicles





Хакеры в автоиндустрии (2017-2018)

2017 BMW /Ford /Infiniti /Nissan Leaf

RCE at Continental AG Infineon TCU

2017 Mobile apps for connected cars research

Research by Kaspersky Lab

2018 aftermarket alarm's backend

Viper Smart/Calamp vulnerability

2018 VW Golf, Audi A3

Computest's research for RCE in IVI

2018 14 vulns discovered in BMW

Research by Tencent Keen security Lab

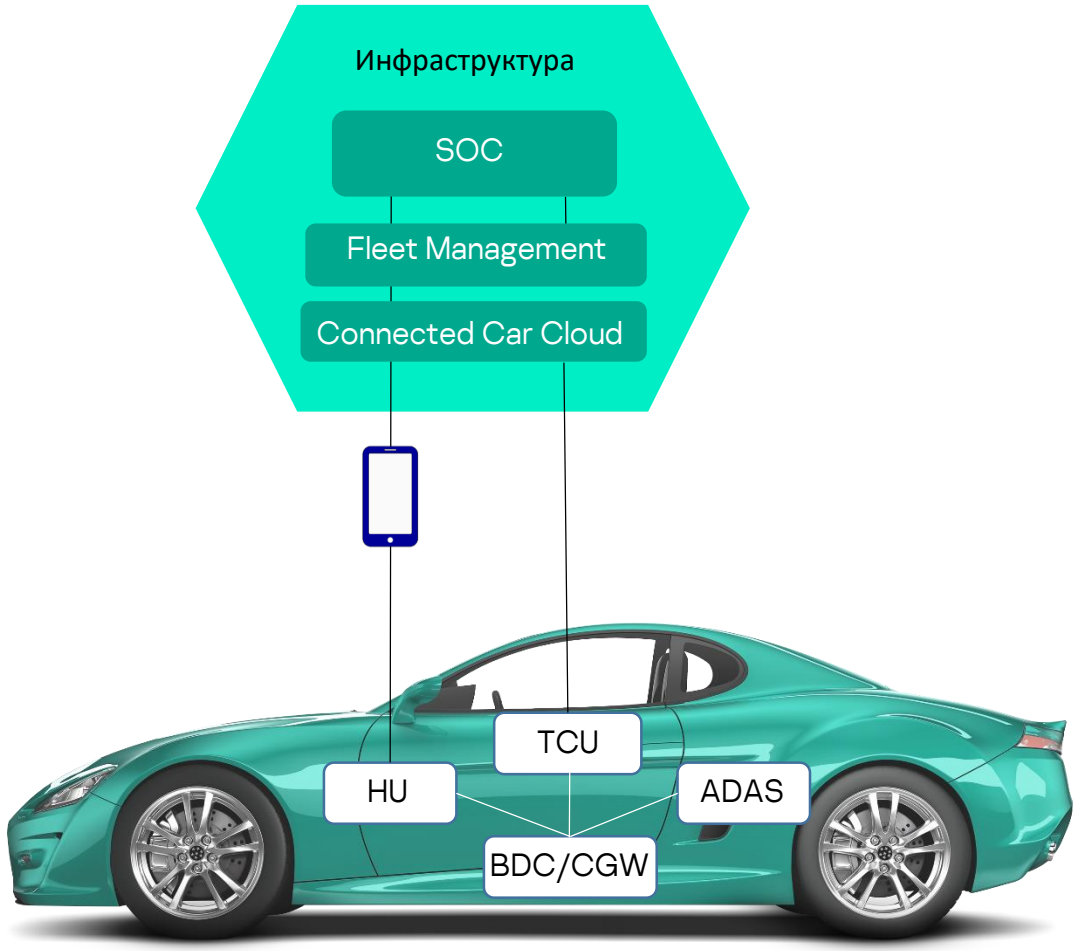
2018 Carsharing application vulnerabilities

Research by Kaspersky Lab

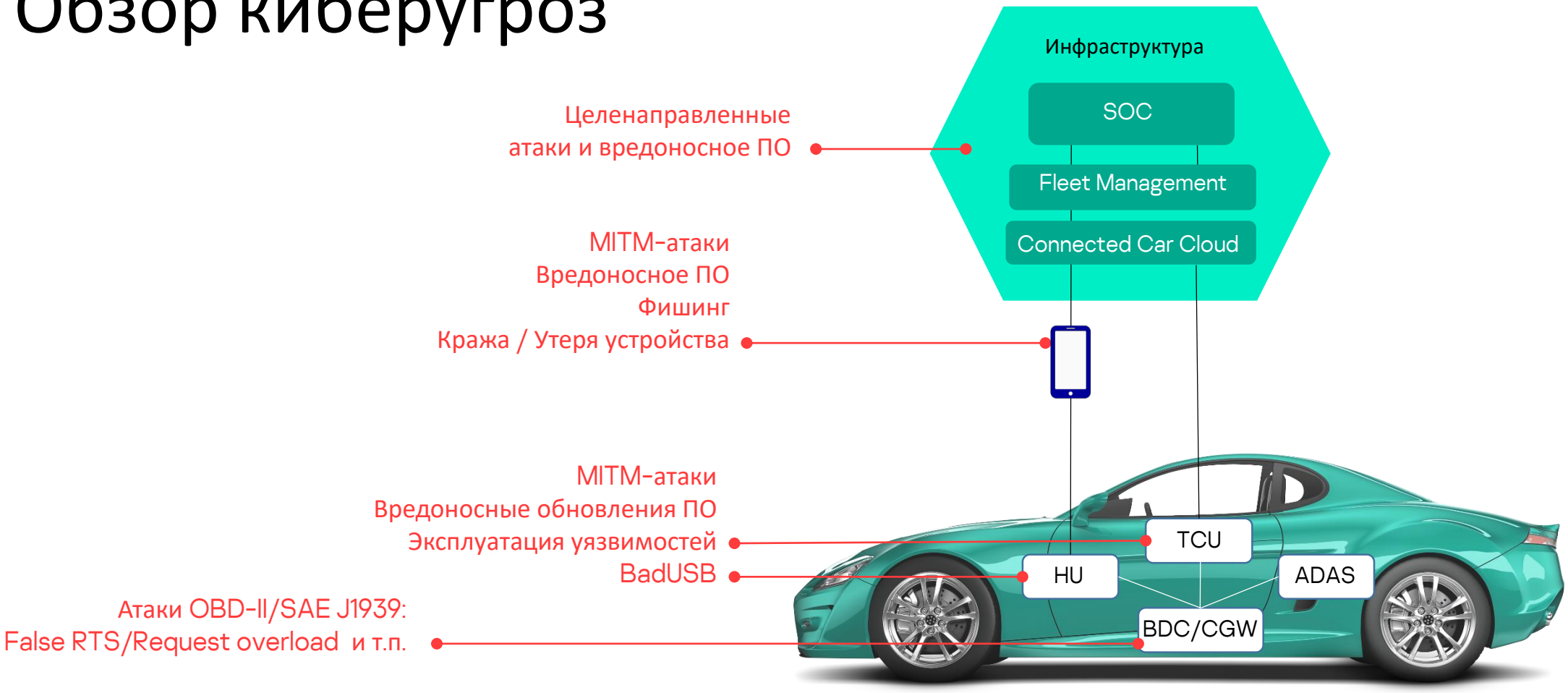
2018 Tesla PKES vulnerability

COSIC experts form KL Leuven University research

Экосистема

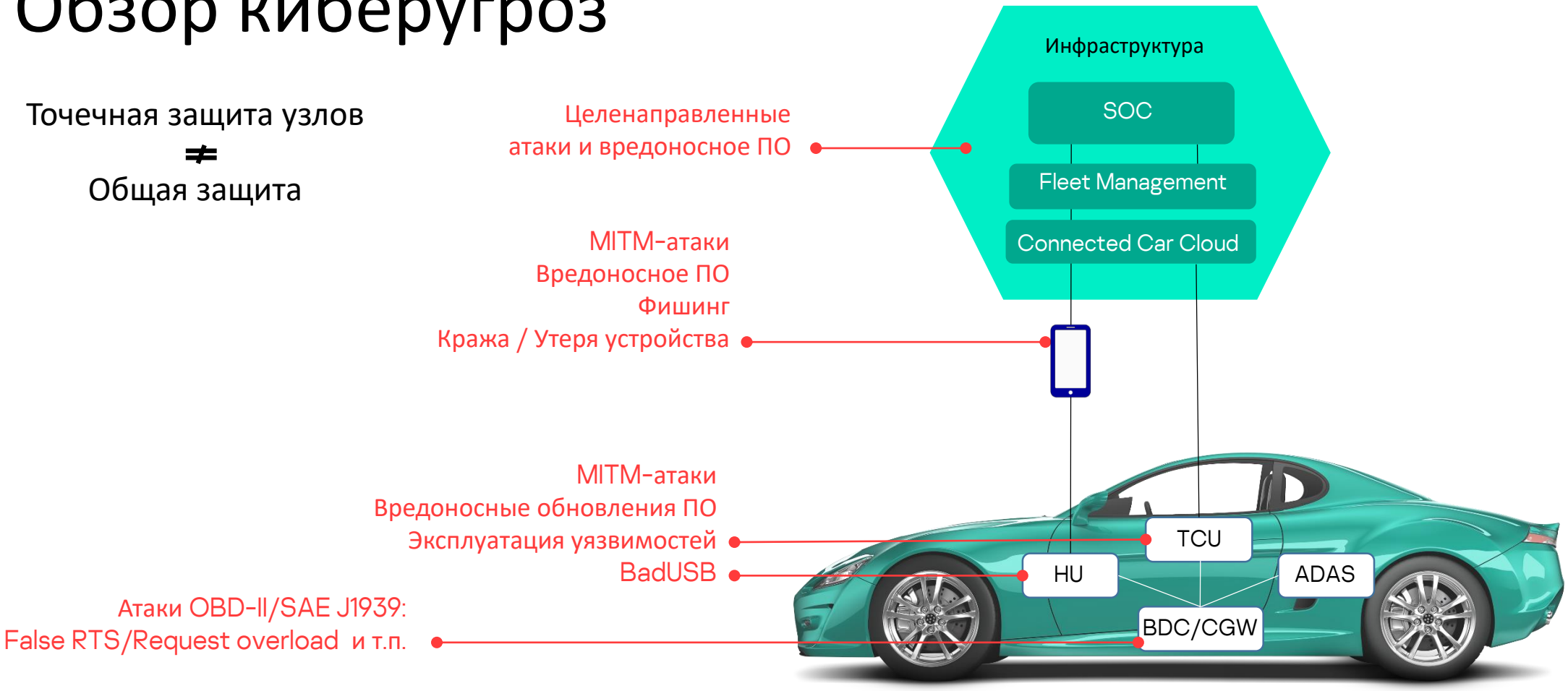

Инфраструктура
SOC
Fleet Management
Connected Car Cloud
TCU
HU
ADAS
BDC/CGW

Обзор киберугроз



Обзор киберугроз

Точечная защита узлов
≠
Общая защита



Развитие **V2X** усложнит экосистему и дополнит список киберугроз

Аудит безопасности мобильных приложений

2016: Лаборатория Касперского протестировала **9** приложений от автомобильных вендоров на устойчивость к ряду кибератак

- Ни одно из них не было защищенным

2017: Лаборатория Касперского протестировала **13** автомобильных приложений

- Лишь одно приложение было защищено и только от одного вида атак

2018: Повтор закрытых тестов **13** автомобильных приложений

- Для **2** приложений завершилась поддержка, и они были удалены поставщиками
- **1** приложение не обновлялось с момента последнего тестирования
- **3** приложения имели какую-то защиту от одного из видов атак
- **10** приложений показали себя не в лучшем виде с точки зрения кибербезопасности

2018: Лаборатория Касперского протестировала приложения для каршеринга

Утечка внутренних данных

Перекрытие приложения

Переупаковка приложения

Недостаточная защита от атак перекрытия
Хранение логинов и паролей в виде простого текста
Отсутствие защиты от реверсинга
Нет проверки целостности кода
Нет обнаружения rooting

Каршеринг и мошенничество

New Android Malware Disguised as Uber App

January 4th, 2018 Waqas Malware, Security 0 comments

It is just another day with just another Android malware targeting unsuspecting users.

Last time Uber was in news for hiding massive data breach of 75 million accounts from its users and paying $100,000 to the culprits. Now, the IT security researchers at Symantec have discovered malware that secretly spies upon Uber's Android app and extracts private, sensitive data such as users' passwords. This allows attackers to hijack the accounts owned by Uber users and

Hackers Steal More Than 100 Mercedes-Benz Cars in Chicago by Hacking Car2Go Car-Sharing App: Report

At least 12 suspects believed to be involved have reportedly been taken into custody.

By Dave Bartosiak

Suspect Arrested for Hacking GoGet Car-Sharing Service

By Catalin Cimpanu • 31 January 2018

Australian police have arrested a 37-year-old man on accusations of hacking GoGet, a car-sharing service.

Police say the man hacked the company last year in May and used access to the company's servers to gain free access to the company's fleet of cars, but also downloaded data on the company's customers from its database.

GoGet only now notifying customers

kaspersky

Подходы к защите транспорта

Kaspersky | Кибербезопасность транспорта: угрозы и меры противодействия

Комплексная защита экосистемы транспорта

Услуги

Аудит безопасности

Тесты на проникновение

Индивидуальный отчет об угрозах

Защита инфраструктуры

Mobile Security SDK

Threat Intelligence data feeds

Портал Threat Intelligence

Защита ТС

Mobile Security SDK

Security for IVI & TCU

Secure Hypervisor

KOS AUTOSAR Adaptive Platform

Обеспечение безопасности (шаг 1)

Обнаружение слабых мест и формулирование требований к разработке

Тест на проникновение (Penetration testing)

Аудит безопасности (Security Assessment)

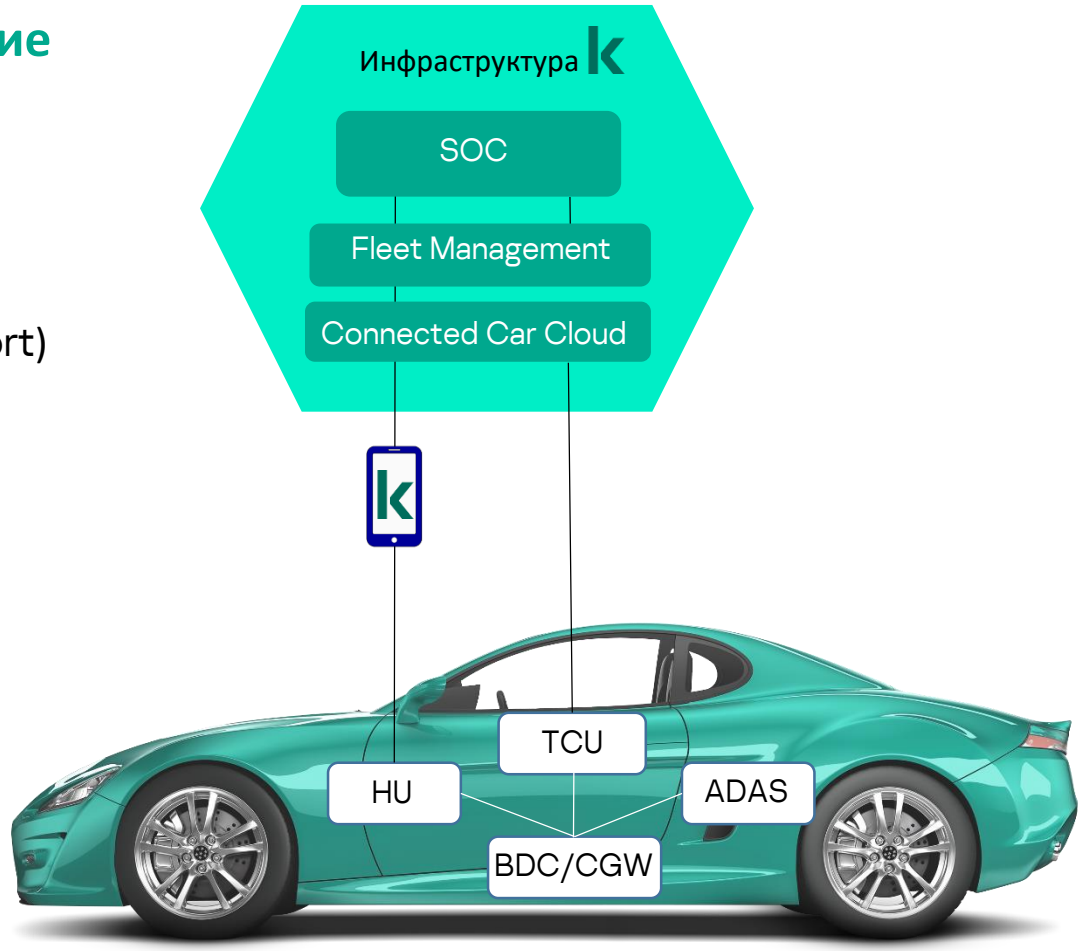
Индивидуальный отчет об угрозах (Custom Threat Report)

Оперативное закрытие известных угроз

Мобильные приложения (Mobile Security SDK)

Инфраструктура (Fraud Prevention, Cloud Security)

Threat data feeds (Threat Intelligence)



Обеспечение безопасности (шаг 2)

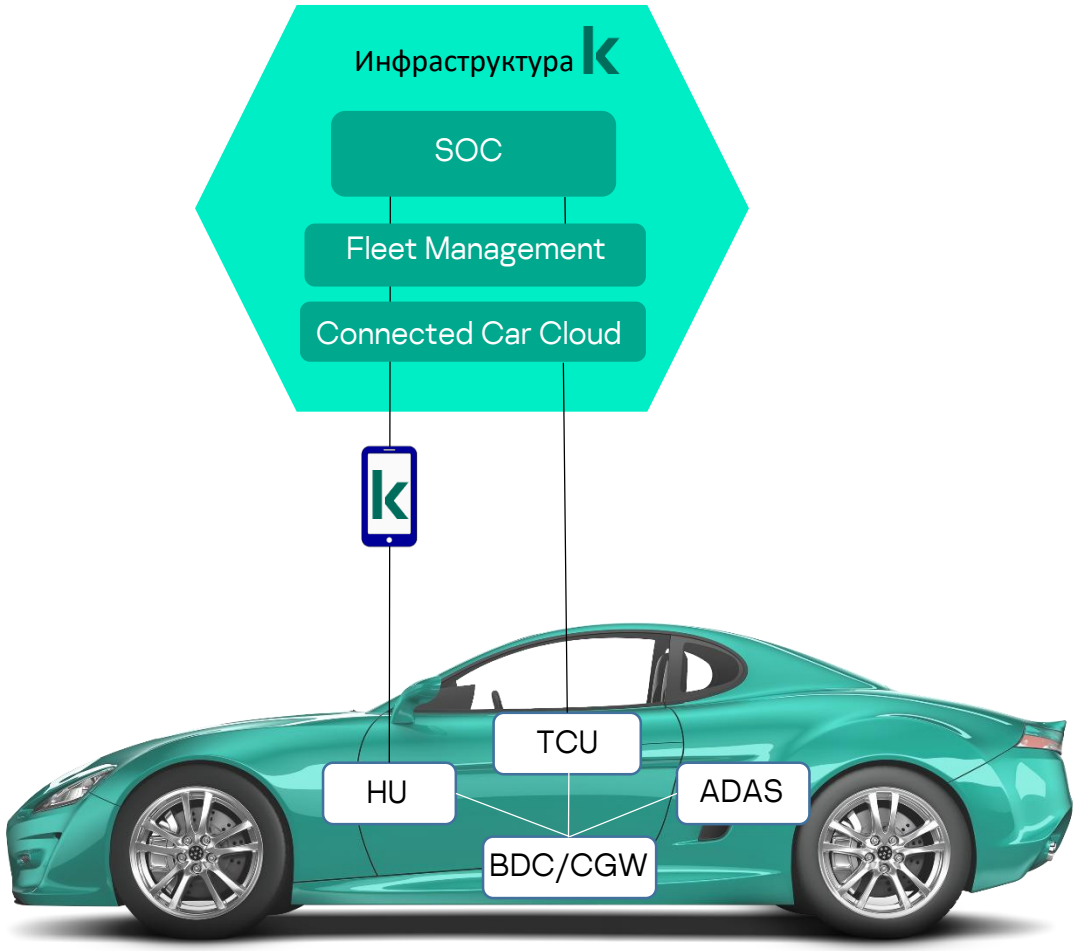
Защита электронных блоков машины и объединение в одну экосистему

Защита для различных ECU

Управление и реагирование

Поставка событий и аналитики в SOC

«Охота» на угрозы и расследование инцидентов



kaspersky

Решение Лаборатории Касперского

Наш подход

Фокус на наиболее критичных блоках ECU

Head Unit

Central Gateway

Telematics Unit

ADAS Platform

Применение технологий защиты

KasperskyOS AUTOSAR Adaptive Platform в качестве слоя защиты

Kaspersky Secure Hypervisor

Дополнительные решения

Контроль портов устройства (Device Port Control)

Контроль коммуникаций (Communication Control)

Контроль приложений (Application Control)

Тестирование и внедрение политик безопасности

Непрерывный мониторинг событий безопасности, связанных с транспортными средствами

Разработка и тестирование политик безопасности

Патчи в существующем программном обеспечении

KasperskyOS AUTOSAR Adaptive Platform

Реализация стандарта AUTOSAR Adaptive

MILS-архитектура (независимых уровней безопасности)

На основе ядра разделения, которое гарантирует контроль всех внутренних коммуникаций системы

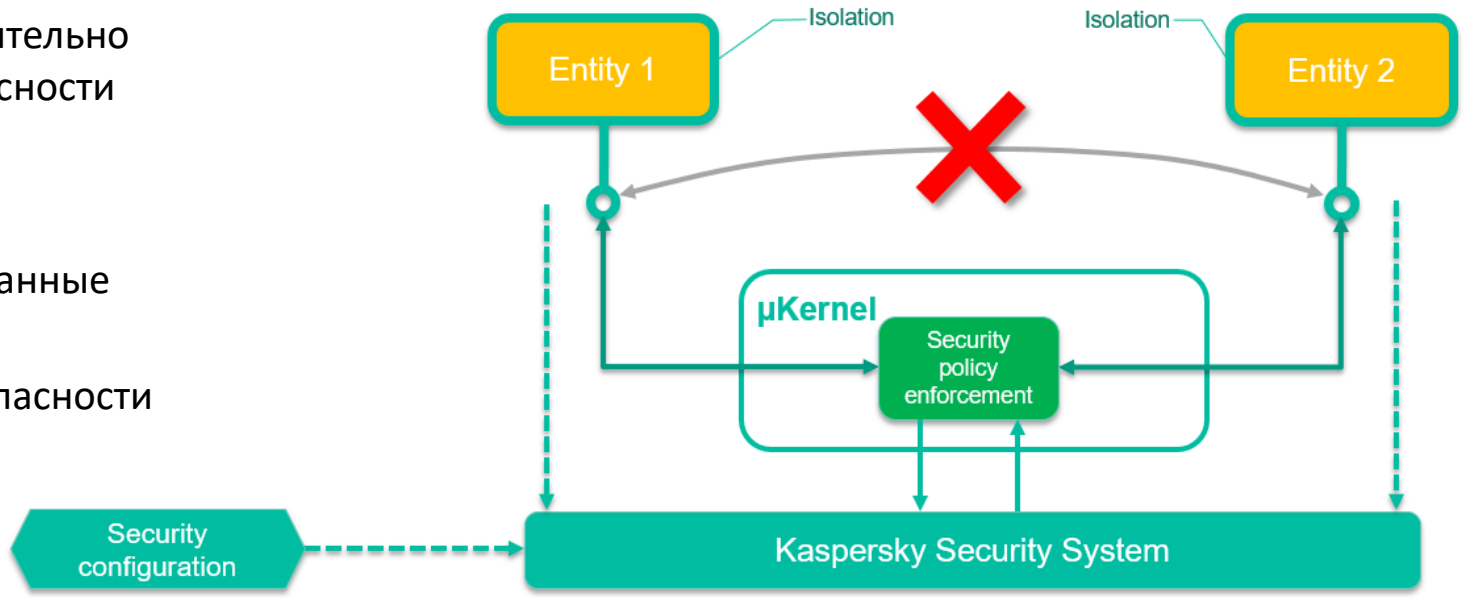
Поведение каждого модуля предварительно описано в политике в области безопасности

- Микроядерная ОС
- Строгая и полная изоляция
- Четко определенные типизированные интерфейсы
- Статическая конфигурация безопасности
- Политика «Default deny»

MILS architecture

Разделение/изоляция доменов

Гибкий контроль внутренних коммуникаций через Kaspersky Security System (KSS)



Компоненты защиты **Kaspersky Mobile Security SDK**

Kaspersky Mobile Security SDK – это модуль для защиты сервисов и мобильных устройств, работающих на операционных системах Google Android, например в Infotainment автомобиля или мобильном устройстве его пользователя.

SDK предоставляет широкий спектр функций для обеспечения безопасности, которые могут быть интегрированы в ваше приложение.

Kaspersky Security for In-Vehicle Infotainment (IVI)

Контроль портов устройств

Антивирусная защита для USB-накопителей (KSN)

Защита от BadUSB-атак

Блокировка внешних диагностических сеансов (OBD-II)

Контроль коммуникаций

Репутация Wi-Fi точек доступа (KSN), защита от атак их подмены

Система предотвращения вторжений (Virtual patching)

Контроль приложений

Hardening приложений, контроль поведения (KSN)

Обнаружение подозрительной деятельности на основе машинного обучения

Интеграция с внешними системами

Противоугонная защита автомобиля (геолокация, блокировка, очистка данных)

Fleet Management systems (местоположение, события)

Интеграция с SOC: «охота» на угрозы и расследование инцидентов

Kaspersky Security for Telematics Control Unit (TCU)

Контроль портов устройств

Антивирусная защита для USB-накопителей (KSN)

Защита от BadUSB-атак

Блокировка внешних диагностических сеансов (OBD-II)

Контроль коммуникаций

Репутация Wi-Fi точек доступа (KSN), защита от атак их подмены

Защита от фальшивых базовых станций

Система предотвращения вторжений
- Virtual patching
- Правила / эвристика / машинное обучение
- Wi-Fi и Bluetooth

Контроль приложений

Hardening приложений, контроль поведения (KSN)

Обнаружение подозрительной деятельности на основе машинного обучения

Интеграция с внешними системами

Противоугонная защита автомобиля (гуолокация, блокировка, очистка данных)

Fleet Management systems (местоположение, события)

Интеграция с SOC: «охота» на угрозы и расследование инцидентов

Kaspersky Secure Hypervisor for ECU consolidation

Гипервизор 2 типа

Isolation guaranties for system resources access

Transparent security control of interacting components

Встроенные механизмы безопасности

Защита страниц физической памяти

Контроль доступа к периферийному оборудованию

Точки обеспечения гостевой политики

Расширенный набор шаблонов безопасности

Доверенная загрузка

Безопасное обновление

Доверенный канал связи

Аудит безопасности

SDK

Настраиваемая политика безопасности

Функциональные модули

Статическая конфигурация

Резюме

Комплексный аудит всей экосистемы

Аудит безопасности бортовых компонентов и связанной с ними автомобильной инфраструктуры

Аудит поставляемых программных модулей для будущих моделей

Релевантные рекомендации по стратегии кибербезопасности

Помощь в выстраивании стратегии
Формирование требований к поставщикам

Интеграция со зрелыми технологиями вендора

Защита ТС и подключенной инфраструктуры

Надежный поставщик кибербезопасности

kaspersky

Спасибо за внимание