

# Trend Micro™ IoT Security for Automotive

Securing Your Connected Vehicle

## NEW TECHNOLOGIES FOR NEW AVENUES

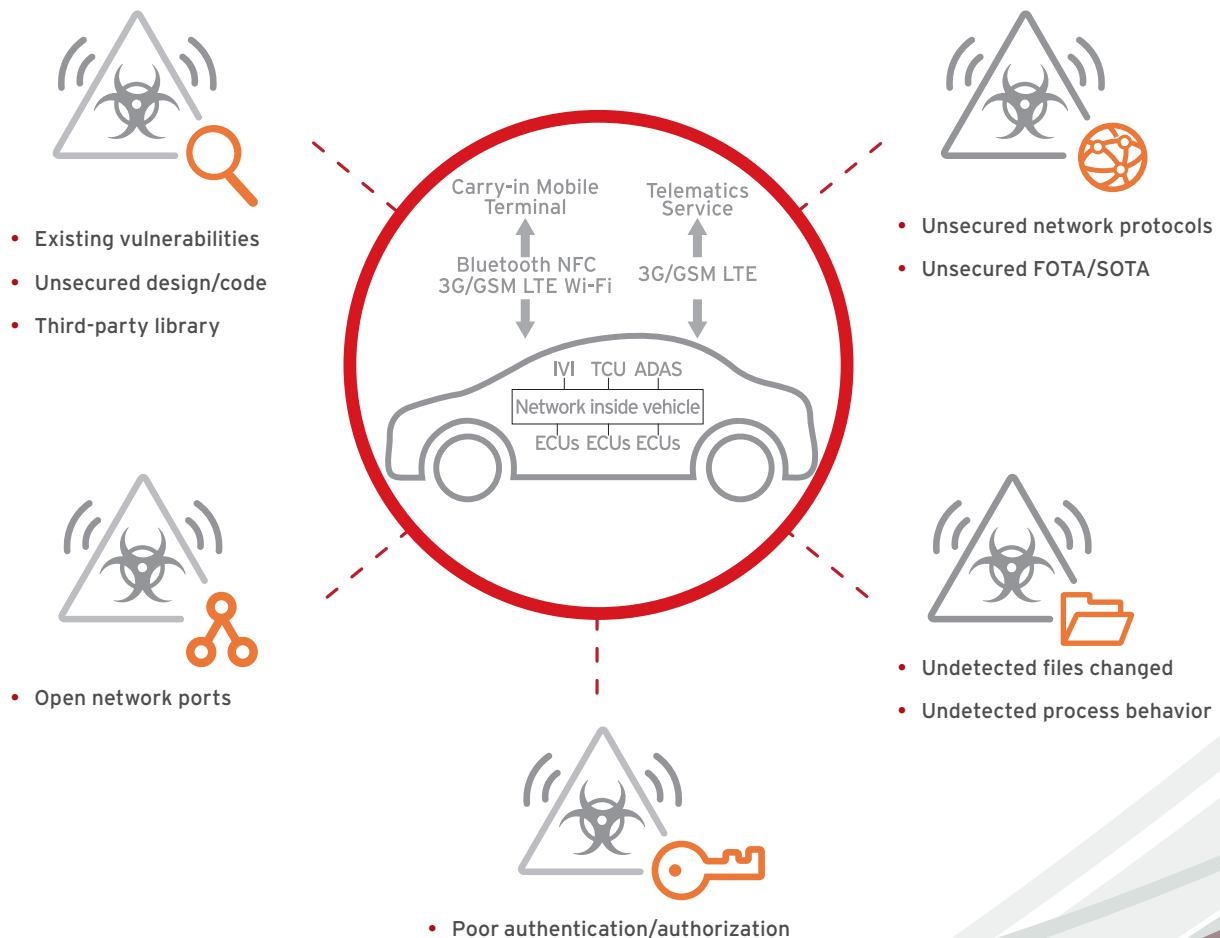
Automotive IoT stands as one of the industry's most revolutionary advancements, allowing vehicles to become smarter, safer, and more efficient. But like any technological development, intelligent and proven security is key to help keep yourself and your data safe from advanced or targeted attacks.

## TREND MICRO IOT SECURITY FOR AUTOMOTIVE

Trend Micro™ IoT Security (TMIS) for Automotive, powered by XGen™, is a built-in security software that monitors and protects critical devices (e.g. IVI) in the vehicle from potential risks, including data theft and ransomware attacks. It ensures system integrity and reduces the attack surface. In doing so, it not only helps keep devices from being hacked, but also minimizes device maintenance costs and protects OEM's reputation.

The design philosophy for connected car security is different from that for the security of other computing systems. Hybrid whitelisting, plus lightware signature-based blacklisting solutions, are suitable because low overhead for a vehicle's system is required. Ensuring device integrity, confidentiality, identification, and operation continuity are all vital when implementing automotive security.

## THREATS AGAINST CONNECTED CAR



## SECURING CONNECTED VEHICLE ENDPOINTS

In order to sufficiently address all possible risks, Trend Micro provides an end-to-end solution for connected vehicle ecosystems. TMIS for Automotive can be integrated (pre-installed) into critical devices inside the car during the product development phase.

As a security sensor, TMIS supports automotive SOC for incident response, which is part of the cybersecurity requirements in the operations phase.

### SYSTEM HARDENING

Checks whether the content of the network belongs to the attack packet and blocks the traffic while ensuring the normal operation of the network.

The virtual patch is used to shield the network from attacks initiated by known vulnerabilities until the vendor is ready to update with the fixed firmware.



The Approved Application List (AAL) feature allows authorized processes and applications to perform certain activities on the device.

AAL policies are automatically generated on local devices (policy is configurable). Supports Block/Monitor mode and works without internet connection.

### RISK DETECTION & WRS

Monitors and matches open-source libraries with CVE's known vulnerabilities. Cloud-based scanning without system overhead in device.

Information about detected vulnerabilities for devices are included in email reports.



When a device tries to visit a URL/website, TMIS performs reputation checks using Trend Micro Web Reputation Services (WRS) to obtain a reputation score.

Configurable whitelist rules to ignore specific IP/domain check.

A deployable detector in the vehicle gateway and an alert for abnormal CAN Bus Anomaly Detection messages were found, including CAN Bus Anomaly Detection ID, frequency, payload structure, and payload sequence. An anomaly log can be uploaded to the backend or the automotive SoC for further analysis or to trigger follow up actions.

## SECURITY REPORTS AND NOTIFICATIONS

TMIS sends the following types of reports and notifications to administrators:

- Device summary
- Security detection information
- License expiration notification
- Vulnerability report
- Virtual patch deployment notification

The security detection log is also saved in local storage and can be accessed by device makers for specific purposes. It allows service providers and device vendors to more easily integrate value-added security features in their offerings.

## TMIS SYSTEM REQUIREMENTS

OS	Embedded Linux® / Android® / Raspberry Pi	Storage	6.7 MB ~ 35.9 MB*
CPU	ARM MIPS X86	Memory	20.4 MB*

\*This data is for reference only. Actual resource consumption will vary according to usage.



Securing Your Connected World

©2019 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: <https://www.trendmicro.com/privacy> [DS\_IoT\_Security\_2.0\_191031US]