Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN R155 Attack Vectors and Beyond

WP.29 is a worldwide regulatory forum within the institutional framework of the United Nations. It penned UN Regulation No. 155, which requires cybersecurity and cybersecurity management systems (CSMS) in vehicles. While the regulation is aimed at manufacturers, its effects cascade to the entire supply chain and is relevant to all connected car stakeholders.

One of its immediate challenges is the need for stakeholders to conduct exhaustive risk assessments to determine what they should prioritize. We provide some guidance in this area. To do so, we used threat modeling to determine the attack vectors' risk levels to help guide stakeholders as they perform their own risk assessments, plan adequate security measures, and subsequently comply with the regulation.

KEY FINDINGS

- At present, focus should be placed on back-end and data security. In the future, risk at the communication channel will dramatically increase.
- Within the next decade, especially with the global rollout of 5G networks, the available technology stack and hacker tools, techniques, and procedures (TTPs) are going to significantly change, and thus the threat profiles and their corresponding risk assessments will also shift.
- While the WP.29 regulatory framework lists an impressive array of cyberattack vectors, we identified additional attack vectors and focus areas, such as image processing attacks and compromised roadway infrastructure.
- Organizations need to first assess the priority of what to focus on and in what order, then determine how to deploy a phased approach to cybersecurity based on that prioritization.

SOLUTIONS

We recommend the following basic principles and expanding from them.

1. Connected car threat intelligence. This is the baseline protection technology that can detect, analyze, protect against, and respond to threats.
2. Multilayered security. The presence of a multilayered security solution would make it increasingly difficult for attackers to succeed.
3. Security covering a comprehensive ecosystem. A comprehensive ecosystem is composed of an endpoint (vehicle), network, and back end.
4. Vehicle Security Operations Center (VSOC). Allows understanding the context of attacks and then take the necessary actions or countermeasures.

Read more about the UN R155-defined attack vectors and our risk assessment by getting a copy of the paper at https://research.trendmicro.com/unr155 and our solutions at https://research.trendmicro.com/CarSolutions.

TREND MICRO | research