CYBERSECURITY FOR CONNECTED CARS

Exploring Risks in 5G, Cloud, and Other Connected Technologies

In this paper, we explore the impact of current and upcoming technologies and risks on connected cars. This research is a continuation of the paper we released last year entitled "Driving Security Into Connected Cars: Threat Model and Recommendations."

Key Findings

- 5G's high-speed and high-quality connections can power **cellular vehicle to everything** (C-V2X), which enables connected cars to react to events around them. Some of the subsets of C-V2X are vehicle to network (V2N), vehicle to device (V2D), and vehicle to vehicle (V2V). In the future, V2X communications will become mainstream and will be used by L3-L5 road vehicles.
- With reliable 5G connections, **some functions from the car's electrical/electronic (E/E) architecture will move to cloud servers** for efficiency. For this, we hypothesize moving data- and processor-intensive electronic control units (ECUs).
- We envision a **cloud-connected ecosystem for connected cars** where the vehicle will be fully integrated with users' digital lives through third-party apps for banking, office work, entertainment, and other uses. The head unit will support a large third-party app ecosystem (similar to mobile phones) and will provide middleware access to the E/E system. This access will enable connected cars to offer innovative add-on features like autonomous ride sharing. Also, machine learning (ML) and artificial intelligence (AI) applications hosted on cloud servers will be extensively used for traffic shaping and predictions. Cloud-specific attacks and middleware APIs (when they are available) will likely become the weapon of choice for cybercriminals.
- **Fleet management** presents cost-saving opportunities for vehicle operators. However, some cybercriminals use the following threats to target fleets: distributed denial of service (DDoS), man-in-the-middle (MitM) attacks, intercept, and fraud.
- For **traditional IT attacks**, we analyzed four remote car-hacking case studies and found an **attack pattern** that was repeated across the attacks. One observation we made is that in all case studies, the hackers attempted some type of MitM attack using either the mobile network or the Wi-Fi network.

Recommendations

In the coming years, we foresee that the number of L3 and L4 autonomous vehicles will dramatically increase, and in a decade, we expect to see L5 vehicles on the road. As the all-digital, feature-rich connected cars become a reality, criminals will invent innovative ways to monetize these vehicles and their resources. The data supply chain will become an important component in the operations and safety of connected cars powered by a fast, reliable network. Automotive cybersecurity technologies should stay ahead of fast-evolving cyberthreats. A multilayered security approach for protecting the vehicle, network, backend, and vehicle security operations center (VSOC) is recommended.

Read more about connected car cybersecurity in our research paper at http://bit.ly/ConnectedCarSecurity.

TREND MICRO | research