Driving Security Into Connected Cars: Threat Model and Recommendations

To shed light on the range of cyberthreats that connected cars face, we analyzed cases of successful remote attacks on connected cars and identified an attack pattern. Our research provides a threat model — with a list of connected car attacks and their corresponding risk levels based on the DREAD (damage potential, reproducibility, exploitability, affected users, discoverability) threat model — to help manufacturers and developers secure connected cars from the early software development stages.

Key Findings

We identified and classified 29 connected car attacks in our threat modeling exercise. We observed that:

About 17% are **high-risk**, about 66% are **medium-risk**, and another approximate 17% are **low-risk**.

The high-risk attacks are the ones that require only a limited understanding of the inner workings of a connected car and can be pulled off by a low-skilled attacker. An example is **discovering and abusing vulnerable remote systems using Shodan**. Shodan is a search engine for internet-connected devices with information that is publicly available and is thus easily accessible to malicious actors, who could use it to find intelligent transportation system (ITS) components that they could compromise.

Sensational attacks, such as **remotely hijacking vehicle controls** and **sending incorrect or improper commands to the back end**, are rated medium- or low-risk. These attacks are difficult to execute because the systems are not readily accessible for attacking, and expert skills and knowledge are required to successfully compromise connected car platforms.

Given their specialized nature, the low-risk attacks, such as **installing malicious firmware over the air**, would realistically affect only a small percentage of everyday connected cars. This is because the attacks are difficult, albeit not impossible, to execute on a massive scale.

Overall, the risk level of **successful attacks on connected cars and ITS infrastructures** is medium. But when middleware that obfuscates the internal electrical/electronic (E/E) car architecture is made available to third-party vendors to provide software as a service (SaaS), we expect to see the emergence of new tactics, techniques, and procedures (TTPs) that will be of a significantly higher risk level. Also, when attackers create viable monetization methods for connected cars and ITS infrastructures, we are bound to see another evolution in their TTPs that will lead to higher-risk attacks.

Recommendations

Tens of millions more autonomous or self-driving cars are expected to hit the roads in the coming decade or two. Cars will become smarter and more connected, and will thus collect and process more data — which means more data for malicious actors to take interest in. In our research, we identified **critical areas in the end-to-end data supply chain** that need to be kept secure. Drawing from our analysis of the risks and threats we identified, stakeholders can develop and implement **a cybersecurity strategy that considers the whole connected car ecosystem** in order to design and build more secure connected cars.

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