GUIDE (BEYOND SECURITY)

How Fuzz Testing Helps Secure the Automotive Industry

As the automotive industry has struggled to make security catch up with innovation, fuzz testing has arisen as a unique solution to some of the industry's more puzzling protection problems. Exploring its unique capabilities will reveal how.

Can Criminals Hijack Cars Remotely?

You are driving for a ridesharing service, when all of a sudden, your electric windows won't roll down. Your passengers in the back are experiencing the same issue. Apologizing for the malfunction, you drop them off and say you'll get it checked out. Insisting it wasn't your fault, they thank you and turn to go – but the doors won't open. Now, things are getting uncomfortable.

You have just been a victim of a remote cyberattack. Your vehicle's connected features have been accessed by hacking the embedded software that powers the doors, windows, steering, and even GPS, giving remote attackers control over the electronic functions of your car. Threat actors are literally holding you and your passengers hostage until the ridesharing service pays the ransom.

While purely hypothetical, such a thing is well within the limits of today and the near future. Without properly testing connected protocols, vehicles today – and the individuals inside – could be just a few clicks away from real risk. Automotive systems have become increasingly more complex, interconnected and prone to cyberattacks in recent years. With larger software bases, multiple external communication interfaces, and more connected IoT features, the attack surface has widened exponentially, exposing drivers to greater risk.

Fuzzing could have helped to prevent the above scenario and works where other methods won't for securing connected vehicle technologies. Let's examine the security problems connected vehicles face and why fuzz testing goes beyond traditional methods to be a particularly useful vehicle cybersecurity tool.

Beyond Safety Belts: What Are We Trying to Protect?

Cars today look more like computers with wheels than the purely mechanical beasts that rolled off Ford's assembly lines. Modern vehicles come with a handful of features that can be vulnerable to risks and threats if not protected. Consequently, protection means much more than the safety offered by a seatbelt.

The first step to protecting modern cars is identifying the connected vehicle features that technology enables, including:

- **IoT-enabled smart features |** This includes services like GPS, vehicle analytics, infotainment, real-time traffic flow analysis, and remote access to emergency features. Also included are hardware devices such as headsets and key fobs.
- **Fleet management |** Another IoT feature, this one warrants specific mention. Today's freight-carrying trucks are equipped with location tracking, weight measurement, and other sensors that store collected information in the cloud. This allows a fleet manager to optimize routes, track road conditions, and keep track of mileage and other performance statistics.
- **Critical embedded software |** Used to manage communication protocols like Wi-Fi, Bluetooth, and Zigbee, embedded software helps divert resources from often over-taxed or limited IoT devices. It also allows for Over-the-Air (OTA) programming that can spare drivers a trip to the dealership by automatically updating software, firmware, and even encryption keys. Mercedes-Benz' recent OTA updates included everything from audio improvements to screen capability. As customizable comforts become more available, critical embedded software and the convenience it brings will be in ever higher demand.
- **Electronic vehicle features |** Your electronic door locks, lights, and other vital functions are operated by a body controller, which responds to radio frequencies such as the ones in your key fob. These frequencies are also used by dozens of vehicular sensors that monitor everything from tire pressure to intra-vehicular communication.
- **Autonomous vehicles |** Autonomous Driving Systems (ADSs) or "the hardware and software that are collectively capable of performing the entire Dynamic Driving Task within its specific Operational Design Domain" are an up-and-coming addition to the driving world, and one that will require critical cybersecurity care.

Overall, exploitable vehicle connections include Vehicle to Infrastructure, Vehicle to Vehicle, Vehicle to Cloud, and Vehicle to Everything (V2X). These massive means of connectivity widen the attack surface and exponentiate the possibility of attack.

Bumps Ahead: The Automotive Cybersecurity Challenges

As even a quick glance at the list above will reveal, the security implications for connected vehicles are enormous. Unsurprisingly, cybercriminals are eager to take advantage of every inroad. Most digital automotive security risks fall into a few camps:

Cyberattacks

Remote hacking, unauthorized access, and resulting malware injection can compromise embedded software and the IoT features that run on it, jeopardizing anything from your GPS system to your brakes, steering, and throttle (not to mention fleet telematics, Advanced Driver Assistance Systems, satellite radio, and everything in between). Denial of Service (DoS) attacks, in particular, can impair a vehicle's ability to interact with other vehicles, the cloud, or the environment by jamming the car's communication channels with moot traffic.

Physical attacks can unlock doors and start cars, using commercially available devices to steal NFC ("near field communication") reader transmissions and illicitly send them via Wi-Fi or Bluetooth to a waiting NFC card. Duping the driver's electronic key with the illegal wireless exchange, attackers can then obtain access to the vehicle (a Tesla, in this case) and drive it until the engine shuts off.

Also problematic in this landscape are the inevitable software vulnerabilities that come with so many moving parts. These include weaknesses in diagnostic systems, entertainment systems, and cloud-connected in-vehicle apps that do everything from finding parking spaces to predicting traffic.

Data Privacy

Connected vehicles collect a lot of data. This is valuable information about the driver's whereabouts, behavior, and even media subscriptions that cybercriminals would love to get their hands on. With stolen driving data, vehicle telemetry, or personal driving preferences, cybercriminals could craft a well-informed phishing email, plan a remote hack on the system, or show up at the driver's expected location with the intent to do physical harm.

"When you buy a car, you're entrusting your automaker [with your information]," noted Darren Mann, vice president of global operations at Seattle-based Airbiquity, and he believes it's the responsibility of the automaker "to make sure that they're treating your data as they should be."

To aid in that process are increasing data privacy regulations like the GDPR and the California Consumer Privacy Act, the latter of which has taken a keen interest in automaker's data privacy practices. However, for the most part, the road to a unified automotive cybersecurity policy remains fraught and fragmented.

AI/Machine Learning Risks

Mostly seen in autonomous transport, the risks involving artificial intelligence and machine learning (ML) within automobiles are still worth investigating. Traffic sign misrecognition (due to vandalism on signs), loss of lane control (in modified or construction-zone lanes), and the inability to avoid objects on the road are some of the bugs still not worked out of the system.

Machine learning is used to perfect autonomous parking (even in non-autonomous vehicles) and spot anomalies on the assembly line, leading to more efficiency in both driving and manufacturing. Currently, data is still largely siloed within different car companies, and the lack of vast amounts of centralized information can hinder the accuracy of potential ML models or at least make training them extremely laborious.

Machine learning is not immune to the actions of threat actors. Just like any other software, ML models can be tampered with. In the case of autonomous vehicles, if the ML models are corrupted, it's could possibly cause the software working off the models to purposely misinterpret a detected object, counter to desired behavior.

The Risk and Reward of 5G

The 5th generation mobile network is designed to boost transmission speed, decrease latency, and generally outperform all iterations before it. And it'd better, because driving decisions need to be made on a dime. For example, Rolls Royce has a production car that plans its gear shifts based on navigating the road ahead via GPS. While convenient, and some might even argue for lightning-fast, the downside is that any latency (or interference) could halt critical operations at a critical time, putting lives at risk.

What is Fuzzing?

Fuzz testing is the automated practice of inputting invalid, unexpected, or random data into a computer program to find errors. The program is then monitored for crashes, memory leaks, or other software defects and vulnerabilities. By putting negative input into the system, fuzzing can detect performance and security gaps by observing the ensuing reaction.

There are several well-known fuzzing methods known in the industry today:

1. **Mutation** creates invalid inputs by randomly mutating valid bits of code.
2. **Replay** mutates already saved sample inputs, then "replays" them to create an attack. However, it does not hold up well in the bidirectional communication protocols found in some automotive systems.
3. **Grammar and generation-based** fuzzing learns the RFC (Request for Comments) and its grammar, then learns what can and cannot be tested by field. While mutation cannot repeat specific attacks on a given field, generation-based fuzzing can. Applying fuzzing to specific parts also speeds the process, as not all packets are immediately blocked by the device under testing, as in mutation, for instance.

Why Other Vulnerability Testing Methods are Insufficient

Fuzzing works particularly well in the automotive industry, providing coverage in the areas in which other solutions fall short. To illustrate, let's examine how fuzz testing stacks up against several different security methods.

Static analysis tools (SAT), used extensively in DevOps environments, need to access the source code in order to spot vulnerabilities. Fuzzing bypasses the source code by testing the communication method and protocol instead. Static analysis would also need to probe into the language of the source code; fuzzing, on the other hand, performs black box testing which requires no special access or information, allowing it to find vulnerabilities in the prerelease stages. As automakers keep proprietary source code close to the chest, third-party fuzzers can safely go in and investigate security issues that other tools would be forced to leave behind.

Machine learning tests the car as a singular operating unit; however, modern connected vehicles are made up of multiple protocols, such as OBDII, CAN, Bluetooth, and Wi-Fi to name a few. Fuzzing can test endless scenarios for each protocol and for many use cases. The ability of fuzz testing to test layers simultaneously adds to its credibility as a unique security tool within the connected automobile industry.

Why is Fuzzing so Effective in the Automotive Industry?

Fuzzers are most effective at uncovering vulnerabilities that can be exploited by attacks such as SQL injection and cross-site scripting, where hackers disable security to steal information or take down a system. Another upside is that fuzz testing can be done during development, much like dynamic application security testing (DAST) and interactive application security testing (IAST).

As vehicle systems have become more complex, fuzz testing has been espoused as a way to combat the new attack vectors that come with larger software bases and an expanded threat landscape. As a result, "the overall cybersecurity engineering process is more comprehensive, security remediation costs are lower, and resources for manual activities such as penetration testing are used more efficiently."

According to one recent report, "Many automotive organizations have made fuzz testing a mandatory step in their software development process or are moving toward doing so." Proven to quickly identify bugs and vulnerabilities, fuzzing has already been integrated into the software development process of industries such as telecommunications.

Conclusion

The automotive industry is becoming more and more digitally connected every day. Automakers need quick and effective ways of testing all specific components of connected vehicles in a secure and timely fashion. Because it can operate in a black box testing environment, test each protocol individually, and quickly distinguish security gaps and vulnerabilities easily exploited by hackers, fuzzing presents a unique and useful solution to staying ahead of the security curve in connected vehicles. Automakers get to test during development without having to reveal their source code, and the vehicle is tested by parts, not as one operational whole (a method that would leave many security stones unturned).

Fortra's Beyond Security BeSTORM Dynamic Application Security Testing Software (DAST) features a black box fuzzing tool that forces automatic code injections to be done from the outside, just like a cybercriminal would do it. Complete your vulnerability assessment by identifying all unknown and undiscovered vulnerabilities, and have access to the following features:

- Compliance assurance: Generate in-depth reports of repeatable findings that can show compliance adherence.
- Efficiently check numerous protocols: Communicate across numerous protocols with prebuilt protocol testing modules.
- Comprehensive QA before release: Make sure your code is properly secure and not easily exploited before it rolls out.
- Fast automated testing: Automate scans during development and monitor after deployment.

Implementing black box fuzz testing will help automakers release their OTA updates with confidence, check multiple systems across connected vehicles, and find the easily exploitable vulnerabilities other tools leave behind.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.