Protecting cars against zero-day attacks

Symantec has introduced Anomaly Detection for Automotive. The solution passively monitors all CAN traffic, learns what is normal behavior, and flags anomalous activity that may indicate an attack.

Connected cars offer drivers conveniences such as navigation, remote roadside assistance, and mobile Internet hot spots. While new technologies promise to enhance the driving experience, these advancements also create avenues of attack for hackers that can endanger drivers and passengers.

Anomaly Detection uses machine learning to provide passive in-vehicle security analytics that monitor all CAN traffic without disrupting vehicle operations, learn what normal behavior is, and flag anomalous activity that may indicate an attack. The solution works with any automotive make and model, claims the manufacturer, and it possesses the ability to identify issues for early remediation, which helps against zero-day attacks.

“The Internet of Things contains many different areas, but connected automobiles will radically alter transportation and mobile communications,” said Christian Christiansen, IDC VP of Security Products. “As connected automobiles become the norm, security issues have already drawn attention. Driven by opportunity, manufacturers and their suppliers will partner with cyber security vendors on securing connected cars as they would with any other networked endpoints such as mobile devices and laptops. Keeping security top of mind will not only help ensure the safety of drivers and passengers but also build trust in the car manufactures and the overall Internet of Things ecosystem.”

The solution learns the vehicle's behavior, enabling automakers to see previously unseen attacks. It automatically prioritizes incidents based on perceived criticality and risk. It also automatically detects anomalies without requiring manufacturers to set rules or create policies. With an analytics solution built from the ground up for vehicles it uses minimal memory and CPU power.

Anomaly Detection for Automotive does not require new hardware. Its small footprint allows multiple deployment options, for example in the head unit, in in-vehicle security gateway modules, as an on-board diagnostics (OBD-II) port device, or any other module where the CAN traffic can be seen. It is compatible with many hardware and operating systems, including embedded platforms.

“Automotive security threats have gone from theory to reality,” said Shankar Somasundaram, senior director of product management and engineering at Symantec. “Symantec is bringing the world's most comprehensive portfolio of security technologies to the car. The infrastructure and technology that already helps protect billions of devices and trillions of dollars now protects the car. We’re building long-term comprehensive security all while delivering ground breaking protection for cars today.”