Karamba Security Launches Autonomous Security for Cars, Empowering Electronic Control Units (ECUs) to Protect Themselves Against Hackers, Including Tesla-type In-memory Attacks

Expanded Carwall product suite addresses Department of Transportation cybersecurity technology guidelines for autonomous and connected cars; blocks recent Tesla-type hacks

HOD HASHARON, Israel and DETROIT, Michigan — Sept. 29, 2016 – Karamba Security today announced Autonomous Security for connected and autonomous vehicles, which empowers their electronic control units (ECUs) to protect themselves from hackers. Autonomous Security, a significant extension to the company's Carwall ECU security platform, enables automotive technology providers to achieve the goals set out in the U.S. Department of Transportation's guidelines for the safe deployment of autonomous cars.

Separately, Karamba Security also announced a new strategic investment round led by Fontinalis Partners, a firm solely focused on investing in and scaling technology companies that are advancing next-generation mobility solutions.

New research from Navigant Research projects that sales of connected and fully autonomous vehicles will grow from 14 million annually in 2020, about 15 percent of annual car sales globally, to nearly 72 million in 2025, accounting for nearly 70 percent of light duty vehicles. By the mid-2020s, they forecast more than 245 million vehicles with level 2 connectivity or higher will be on the road.

In the report, "Autonomous Automotive Cybersecurity," Senior Research Analyst Sam Abuelsamid concludes solving cybersecurity problems, however, is critical for achieving this forecast, and one key risk he singles out is the probability of having false positives. With today's network-based approaches, approximately two of every 100 commands suspected as malicious on the car's CAN bus network will be mistakenly blocked. "The fatality risk of such frequent blocking of valid operations is something the automotive industry cannot tolerate," he said.

Karamba Security's automated ECU technology eliminates this risk by providing zero false positives.

Stephan A. Tarnutzer, vice president, Electronics at FEV North America, Inc., a Tier-1 global automotive supplier and internationally recognized powertrain and vehicle engineering company, agrees with Abuelsamid that preventing false positives is a critical point.

"Experiencing false positives or detecting hacks on the CAN bus, only after the fact, are unacceptable risks in vehicle engineering," said Tarnutzer. "FEV North America works with Karamba Security because we've seen the benefit of its Autonomous Security technology in securing our own ECUs. Karamba's technology doesn't require any developer resources to install or generate the security policy, and its CPU footprint is negligible. We are working

with Karamba to integrate Carwall into our reference platform, which will allow us to present our automotive customers with a secure system out of the box."

How Carwall Autonomous Security works

Cyberattacks can only infiltrate a car by compromising the externally-connected ECUs controlling infotainment, navigation and OBDII telematics dongles, for example.

Karamba Security's Autonomous Security technology allows any car's ECU to protect itself from this threat by automatically locking it down to the ECU's factory settings. The ECU then blocks operations that aren't part of its factory settings, with a negligible performance impact, which prevents hackers from accessing the car's safety systems and commandeering them.

This deterministic decision is made locally on the ECU. Autonomous Security doesn't require the ECU be connected to protect itself, nor does it need anti-malware updates.

Today, Karamba Security also unveiled a new capability, in-memory protection, as part of its Autonomous Security suite. With in-memory protection, the ECU autonomously blocks memory-based attacks such as buffer overrun and return oriented programming (ROP).

In-memory Autonomous Security blocks common in-memory attacks, such as the Tesla hack demonstrated last week. With its recently announced security upgrade, Tesla has stated that it tried to make it harder for hackers to reprogram other ECUs once they've compromised the externally connected ECU. In effect, Tesla's approach accepts that hackers will penetrate the car's ECU and then tries to minimize the damage. In sharp contrast, Karamba Security in-memory protection blocks such hacks altogether. Specifically, the attack demonstrated by the researchers would have failed in Teslas or any vehicle protected by Carwall.

Since Karamba Security's Autonomous Security works by locking down the ECU to instructions that are known to be good, it does not have to "guess" about a command it may not have seen before, thus avoiding the risk of false alarms, or false positives, inherent in other approaches. False positives can lead to legitimate car commands failing to execute, consequently risking lives.

"The risk of a car hack is lost lives," said Ami Dotan, CEO and co-founder of Karamba Security. "Any security approach that's vulnerable to false positives or delayed decision-making isn't providing sufficient security. ECUs have to be able to protect themselves to prevent intrusions. Karamba's Autonomous Security hardens ECUs with a complete security solution that no one else offers."

Five months after emerging from stealth with its Carwall automated ECU security platform for connected cars, Karamba Security has completed technology proof of concepts with several industry Tier-1 providers and has been experiencing strong demand for its Carwall product suite from car OEMs and Tier-1 providers.

Karamba Security will be speaking at multiple industry events this fall, sharing its Autonomous Security framework and why its prevention and performance advantages make it the only security solution that rises to the level of risk connected and autonomous vehicles face.

- GENIVI Alliance All-Member Meeting (Burlingame, California, Oct. 18-21)
- Automotive Cyber Security Summit West (San Francisco, Oct. 24-26)
- Driverless Cities (San Mateo, California, Oct. 26- 28)
- TU-Automotive Cyber Security (Munich, Nov. 2-3)
- ESCAR Europe (Munich, Nov. 16-17)

# # #

Resources
Navigant Research Report: Autonomous Automotive Cybersecurity
Karamba Security Autonomous Security FAQ
Karamba Security Autonomous Security Chart
Karamba Security Carwall Animation

About Karamba Security

Karamba Security provides industry-leading autonomous cybersecurity solutions for connected and autonomous vehicles. Karamba's software products automatically harden the ECUs of connected and autonomous cars, preventing hackers from manipulating and compromising those ECUs and hacking into the car. Karamba's Autonomous Security prevents cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. More information is available at www.karambasecurity.com.