Karamba Security and FEV Demonstrate at CES
How to Keep Self-Driving Cars Safe from Hackers

HOD HASHARON, Israel and ANN ARBOR, Michigan — December 27, 2016 – Karamba Security, a provider of zero false positive autonomous cybersecurity solutions for connected and autonomous vehicles and FEV, a leader in the development and testing of electronics systems and subsystems for Advanced Driver Assisted Systems (ADAS), have partnered to demonstrate how their joint cybersecurity technology solutions can keep self-driving cars safe from hackers.

The demonstration will take place during CES in Las Vegas, Jan. 5 – 8, 2017 at FEV's Bellagio Hotel suite.

Karamba's software enables electronic control units (ECUs) to autonomously protect themselves from hackers. It automatically hardens car ECUs, preventing hackers from compromising those ECUs and hacking into the car.

How Hackers Attack

Attackers try to inject malicious messages designed to modify a vehicle's behavior, either by a local or remote attack. The industry responded by trying to use network anomaly detection systems, also called Intrusion Detection Systems (IDS), that monitor the on-board communication bus (CAN) to detect anomalous messages, which may indicate an on-going attack. The results, however, have been problematic, according to industry experts.

"These systems usually deploy heuristic methods, and hence raise false alarms (false positives) and miss attacks (false negatives)," according to Dr. André Weimerskirch, an industry expert in the field of vehicle electrical systems and cybersecurity, most recently with the University of Michigan and now vice president of Cyber Security with Lear Corporation's E-Systems team.

In his presentation at the October 24 – 26, TU 2016 Automotive Cyber Security Summit in San Francisco, Dr. Weimerskirch stated that as a result, it seems unreasonable to use any heuristic-based prevention in the vehicle in the near future. Since there will always be some false alarms, he argued, and if that were to trigger an active prevention, it might have an impact to safety relevant systems, without any on-going attack. Thus, anomaly detection systems do not replace prevention mechanisms, such as network separation, firewalls, and secure CAN, he concluded.

In 2016 Karamba Security emerged from stealth to solve this problem. Within three quarters, the company's Autonomous Security product is being evaluated with eight different proofs of concept, and in the pipeline are dozens of other companies, owing to the advantages Autonomous Security brings to the car industry:

- A software solution that prevents cyberattacks with zero false positives, eliminating the risk of safety impacts
- No malware updates required
- Automatic policy generation with zero development efforts

“Detection is not enough, if the industry is going to put the brakes on hackers targeting connected and autonomous vehicles,” said Ami Dotan, CEO of Karamba Security. “The market shows strong interest in a solution aimed at prevention, with zero false positives, like Karamba’s Autonomous Security.”

# # #

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.