Karamba’s Autonomous Security Meets New NHTSA, U.S. DOT Guidance for Automated Driving Systems Safety and the SELF DRIVE Act

ANN ARBOR, Mich. and HOD HASHARON, Israel — Sept. 12, 2017 – Karamba Security, a provider of cybersecurity solutions for connected and autonomous vehicles, today announced that Karamba’s Autonomous Security enables automotive technology providers to meet the goals set out in the National Highway Traffic Safety Administration (NHTSA) and U.S. Department of Transportation (DOT)’s newly published federal guidance, *Automated Driving Systems (ADS): A Vision for Safety 2.0*, led by U.S. Transportation Secretary Elaine L. Chao—as well as the guidelines defined in the SELF DRIVE Act passed by the U.S. House of Representatives last week.

According to the NHTSA and U.S. DOT, “A Vision for Safety seeks to facilitate the integration of ADS technology by helping to ensure its safe testing and deployment, as well as encouraging the development of systems that guard against cyberattacks and protect consumer privacy.”

The federal guidance also says, “Vehicle Cybersecurity Entities are encouraged to follow a robust product development process based on a systems engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities.”

“This encourages manufacturers to do security by design in accordance with Karamba’s approach. The new federal guidance emphasizes software development, verification and validation, but after all that, you still have bugs in software,” said Ami Dotan, CEO and co-founder of Karamba Security. “By automatically hardening the controllers with Karamba’s technology as part of the software release process, you make sure that even when hackers identify hidden security bugs, those bugs are not exploitable. This approach strengthens the concept that the NHTSA and U.S. DOT recommend the industry comply with— which is to remove as many security vulnerabilities as possible and ensure that the vulnerabilities that still remain will not be leveraged by the hackers, risking consumer safety.”

Karamba’s Autonomous Security software seamlessly protects connected and autonomous cars by hardening electronic control units (ECUs) based on their factory settings. This is the industry’s first prevention solution with zero false positives, because it blocks deviation from the ECU’s factory settings, i.e. malware.

Applying software engineering rules of thumb, Karamba estimates that the software for premium connected and autonomous vehicles’ ECUs contains up to 60,000 bugs – including 5,000 security defects. These bugs potentially allow malicious hackers to take over the ECU, which is connected to the internet and external networks, and manipulate critical components such as steering and brakes.

“The best way to maintain consumer safety and block hacking attempts is to ensure that only factory settings are allowed to run on the car’s attack surfaces, which are the externally-connected ECUs. With Karamba’s technology, every unauthorized change to factory settings is deterministically blocked, with zero false positives. Such an approach enables the automotive industry to address U.S. DOT and NHTSA’s and the SELF DRIVE Act’s guidelines, while maintaining consumer safety,” said Dotan.

The SELF DRIVE Act

The SELF DRIVE Act is first-of-its-kind legislation to ensure the safe and innovative development, testing and deployment of self-driving cars. While self-driving technology is currently being developed and tested across the country, from Silicon Valley to Detroit, federal motor vehicle safety standards need to be updated to reflect cars without traditional design features.

According to Section 5, CYBERSECURITY OF AUTOMATED DRIVING SYSTEMS, of the SELF DRIVE Act passed by the U.S. House of Representatives, a manufacturer may not sell, introduce, deliver or import into the U.S., any highly automated vehicle that performs partial driving automation or an automated driving system unless such manufacturer has developed a cybersecurity plan. That plan must include a process for identifying, assessing and mitigating reasonably foreseeable vulnerabilities from cyberattacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands; and a process for taking preventive and corrective action to mitigate against vulnerabilities in a highly automated vehicle or a vehicle that performs partial driving automation, including incident response plans, intrusion detection and prevention systems that safeguard key controls, systems, and procedures through testing or monitoring, and updates to such process based on changed circumstances.

Since coming out of stealth at the end of March 2016, Karamba Security has been actively engaged with 16 different ECU-hardening projects throughout the industry with car manufacturers and Tier-1 providers. In addition, Karamba was unanimously recognized with TU-Automotive's Best Cybersecurity Product/Service and the 2017 North American Frost & Sullivan Award for Automotive New Product Innovation.

More information is available at www.karambasecurity.com.

Resources
Autonomous Security
Karamba Security Approach
Karamba Security FAQ

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. In one year, Karamba has received a total investment of $17 million. The company has been recognized in 2017 with TU-Automotive's Best Cybersecurity Product/Service and the North American Frost & Sullivan Award for Automotive New Product Innovation. More information is available at www.karambasecurity.com.