Karamba Security Launches End-to-End Automotive Authentication with Zero Network Overhead

BLOOMFIELD HILLS, Mich. and HOD HASHARON, Israel — Dec. 12, 2017 – Karamba Security, the world leader in automotive cyberattack prevention, today announced SafeCAN, its new security software that seamlessly protects automotive networks from hacking by authenticating in-vehicle communications with zero network overhead.

Carmakers have been demanding authenticated in-car communications to protect vehicles against malicious messages sent by unauthorized Electronic Control Units (ECUs) or via third-party dongles. Such prevention is essential in light of dongles commonly provided by insurance companies to monitor driver behavior and offer discounted premiums to responsible drivers. Car companies can't control the data exchange generated by those dongles, creating a new attack vector. A Toyota car model was compromised by researchers through a dongle from Progressive Insurance, for example.

Solving this problem is made even more difficult because in-car networks, and especially the CAN bus, are saturated and cannot add authentication data, which consumes network throughput. The resulting lack of in-car authentication leaves the car's safety systems exposed to malicious commands sent due to such dongle-based attacks or hacked over-the-air (OTA) in-vehicle updates.

"Authenticating car networks is an urgent and important matter that the automotive industry has been coping with for several years," said Miroslav Pajic, assistant professor in the Department of Electrical and Computer Engineering at Duke University. "Saturated car networks created technological barriers in finding a solution that will authenticate all traffic to and from the car's safety systems, such as brakes and airbags, exposing them to physical and cyberattacks."

SafeCAN is the automotive industry's first cybersecurity solution to offer in-vehicle network authentication with zero network overhead. It can be implemented without overtaxing the car's internal communications to protect and authenticate CAN bus communications.

Karamba's latest software product enables automobile manufacturers to seamlessly harden the networks to secure the car's safety systems. There is no need to change network protocols, or add any additional network packets to ensure the authenticity of source-destination authentication and overall in-vehicle network authentication.

By offering seamless encryption for ECU communication, SafeCAN hardens the network leading to and from the car's safety systems and ensures that only legitimate commands are received by the car's safety systems. Commands originating from invalid sources are ignored.

In addition to hardening the car networks against physical attacks, SafeCAN enables secure OTA updates from the cloud to any ECU in the car. OTA products use secure channels from the OEM cloud to the primary ECU, which serves as the OTA's entry point in the car. However, due to lack of network authentication, attackers may hack the car, impersonate an OTA update and deploy malicious software on safety ECUs. By hardening the network between the OTA primary ECU to the in-vehicle safety systems, target ECUs will not accept changes, unless it was authenticated by SafeCAN.

This marks the first time that any vendor has offered end-to-end network safety in a pragmatic way that overcomes industry barriers.

"Karamba Security's SafeCAN addresses the industry's need to authenticate in-vehicle communication, to protect safety systems against hacks, and to ensure that OTA updates are not used to deploy malware on target ECUs," said Roger Lanctot, Director Automotive Connected Mobility at Strategy Analytics.

SafeCAN helps automakers and tier-1 providers meet their security goals and comply with regulations such as those set out in the United States by 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, as well as the guidelines defined in the SELF DRIVE Act passed by the U.S. House of Representatives. Similar guidelines are emerging worldwide.

"We listened to our OEM customers, and innovated to meet the challenges they identified with the unsolved problem of in-car communication security," said Ami Dotan, CEO and co-founder of Karamba Security. "Car manufacturers are concerned with physical hacks as well as the use of OTA technology to get secure cloud-to-vehicle communications, but their security ends at the entrance to the car. We cover the last yard, communication to and from safety ECUs, to make sure only legitimate messages from any entry point are accepted throughout the car network, and that safety will not be compromised."

SafeCAN complements and extends Karamba's Autonomous Security Carwall product to provide end-to-end in-vehicle security. Carwall hardens externally-connected ECUs by sealing their binaries according to factory settings. This prevents cyberattacks and in-memory attacks from compromising the car ECU's, while eliminating false positives that risk consumers' safety.

Together, SafeCAN and Carwall assure car safety by blocking hackers at the gate and by providing secure in-car traffic and authenticated OTA updates.

Karamba will be at CES® 2018 January 9-12, 2018, in Las Vegas, Nev. to showcase its capabilities working with leaders in the global automotive supply chain. From its suite at the Bellagio Hotel, Karamba will conduct joint demonstrations with partners who include Honeywell, IAV, Alpine and FEV to engage with conference-goers on cybersecurity vulnerabilities and how

organizations can work together to secure the automotive industry. To schedule a private demo email: ces@karambasecurity.com.

Since coming out of stealth at the end of March 2016, Karamba Security has been actively engaged with 16 different car makers and tier-1 providers on hardening their ECUs of choice.

In November of 2017 Karamba Security was named by CNBC to its list of most innovative startups. In addition, Karamba Security was unanimously recognized with TU-Automotive's Best Cybersecurity Product/Service for 2017 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

About Karamba Security
Karamba Security provides industry-leading cybersecurity solutions for connected and autonomous vehicles. Its SafeCAN and Carwall software provide end-to-end in-vehicle security by authenticating communications, including OTA updates, with zero network overhead and by hardening the car's safety ECUs from attempts to manipulate or compromise their commands and hack into the car. Together, the products prevent cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. In one year, Karamba has engaged with 16 OEM and tier-1 customers, 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.