Karamba Security Announces Collaboration with Micron for Enhanced Automotive Cybersecurity

Karamba ECU hardening and CAN Bus encryption software will utilize Micron® Authenta™ Technology to deliver a stronger layer of defense to automotive systems

TU-AUTOMOTIVE DETROIT – June 5, 2018 – Karamba Security, a world-leading provider of end-to-end automotive cybersecurity prevention solutions today announced a new industry collaboration to enhance security hardening for the automotive market. Karamba Security is working with leading semiconductor vendor Micron Technology to leverage the Micron® Authenta™ security architecture in Karamba's Electronic Control Unit (ECU) hardening and CAN Bus encryption software, enabling an enhanced embedded security solution previously unavailable for traditional in-vehicle architectures. This solution will leverage hardware security features in Authenta-enabled flash memory to improve content and run-time integrity while simplifying overall platform security implementations.

"Micron is a leading provider in the connected car ecosystem," said Ami Dotan, Karamba Security's co-founder and CEO. "When looking at the emerging autonomous vehicle architecture we all know security needs to be enhanced. We are proud to join forces with Micron to improve out-of-the-box security when hardening crucial in-vehicle units to ensure consumer safety."

"Cybersecurity has become a critical concern for our automotive customers as the market transitions to the era of connected vehicles and emerging autonomous vehicles. Cybersecurity issues are complex and require a combination of hardware and software technologies to be closely integrated to simplify implementation, adoption and solution hardening," said Giorgio Scuro, vice president of the Automotive Division at Micron. "We are pleased to team with Karamba, who has a strong fit with our Authenta security ecosystem, and who shares our vision of simplifying adoption of enhanced security solutions by our customers."

The Karamba technology integration with Micron leverages industry-standard cryptographic primitives in silicon available uniquely on Micron's Authenta-enabled flash memory. When Karamba automatically creates a security policy for run-time integrity validation and binary whitelists, it leverages the Authenta-enabled flash memory device to attest to the integrity of these critical elements through authenticated commands and cryptographic measurements. This advanced implementation provides a higher level of resiliency while keeping the performance level the industry has come to expect from Karamba hardening solutions.

Key advantages for this announcement:

- Out-of-the-box integration between Karamba end-to-end protection and Micron® Authenta™ security architecture

- Higher level of security and resiliency while maintaining 100 percent of Karamba's software real-time prevention capabilities against zero-day exploits

- Zero false positives; no lengthy process of detect-investigate-respond for critical attacks

- Seamless and rapid integration into any ECU code, without developer intervention, avoiding time-to-market delays

- Trustworthiness of critical code and policy data based on silicon roots of trust and built-in measurements in Authenta-enabled flash devices

- Security hardening leveraging flash memory—a socket that already exists in all main automotive electronic platforms—eliminating need to add additional hardware components for security and reducing architectural fragmentation

Recently, Karamba Security was selected by Gartner as a Cool Vendor for IoT Cybersecurity 2018 where its automotive track record was considered an important factor for the technology potential in other verticals.

Visit Karamba Security at TU-Automotive Detroit on June 5-7, booth B143, to see the latest from Karamba and learn more about this enhanced security solution leveraging Micron Authenta technology.

About Karamba Security
Karamba Security provides industry-leading automotive cybersecurity solutions for autonomous and connected cars. Its autonomous security software products, including Carwall and SafeCAN, provide end-to-end in-vehicle cybersecurity for the ECU and the internal messaging bus. Karamba Security's award-winning solutions prevent zero-day cyberattacks with zero false positives and secure communications with negligible performance impact and seamless integration into the car software. Karamba, with headquarters in Michigan, is engaged with 17 OEM and tier-1 customers and received numerous industry awards. More information is available at www.karambasecurity.com.

Karamba Security Business Contact:
Amir Einav, VP of Marketing
amir.einav@karambasecurity.com
214-620-7320

Media Contact:
Montner Tech PR
Deb Montner
dmontner@montner.com
203-226-9290