CAN Newsletter Online

COLLABORATION

Enhanced automotive cyber security with CAN

The Karamba ECU hardening and CAN encryption software will utilize the Micron Authenta technology to deliver a stronger layer of defense to automotive systems.

CAN in Automation offers cyber security workshops (Photo: Fotolia)

Karamba Security is working with Micron Technology to leverage the Micron Authenta security architecture in Karamba's Electronic Control Unit (ECU) hardening and CAN encryption software. This enables an enhanced embedded security solution 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, said the company. The Authenta technology provides a level of protection for the lowest layers of IoT device software, starting with the boot process. The approach of utilizing existing standard flash memory sockets enables system developers to harden system level security without adding additional hardware components.

"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."

"Cyber security has become a critical concern for our automotive customers as the market transitions to the era of connected vehicles and emerging autonomous vehicles. Cyber security 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 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. This attests the integrity of these critical elements through authenticated commands and cryptographic measurements. The cooperation enables seamless integration into any ECU code, without developer intervention.

cw