Karamba Security Hardens Vector MICROSAR-based ECU Software to be Self-Protected Against Cyberattacks

Stuttgart, Germany and Hod Hasharon, Israel - 12 September 2019 – Karamba Security, a global leader in embedded cybersecurity solutions, today announced that it successfully applied its Control Flow Integrity (CFI) technology for the first time on ECU software that is based on Vector's leading Classic AUTOSAR solution MICROSAR. Vector is one of the leading suppliers of software tools and components for the development of electronic systems in vehicles and one of the most important suppliers of AUTOSAR basic software in the automotive industry.

How CFI works in ECU Software

Karamba Security's embedded security technology enables ECUs to automatically protect themselves against external attacks. It seamlessly seals function calls and function returns according to factory settings and prevents hacker attacks without the risk of false positives. This deterministic approach prevents file-less attacks from exploiting buffer overflow vulnerabilities and other in-memory vulnerabilities. Without the need for continuous malware signature updates and costly Over The Air updates mechanism, Karamba Security Carwall® provides CFI protection to vehicles' ECUs against manipulation attempts and harmful commands from outside.

"Through the integration of Karamba Security's CFI into the MICROSAR-based ECU software, automobile manufacturers receive a fully hardened component that automatically protects itself against even the most sophisticated attacks," explains Tal Ben David, co-founder and VP R&D of Karamba Security. "This integration simplifies the introduction of embedded security and saves time and money for the Electronic Control Unit (ECU) developers. They can now use an automatically hardened ECU software that is based on Vector's Classic AUTOSAR stack and receive support for all applications that dock to it."

Automotive industry prepares for cyber attacks

Cybersecurity is one of the major priorities for the automotive industry. The market is growing: It is not for nothing that analysts from Markets & Markets predict that the global market for automotive cybersecurity will grow from around 1.34 billion US dollars today to 5.77 billion US dollars in 2025. For good reason: the increasing number of interfaces between vehicle systems makes critical components that guarantee functional security vulnerable to cyberattacks.

Consumers are becoming more and more aware of the cyber risks to connected systems: In a recent Karamba Security survey carried out in Germany, 80% of respondents said that one of their biggest cybersecurity concerns for connected vehicles is that critical safety functions could be hacked, causing malfunction or an accident.

Implementing CFI can help to improve functional safety and is also recognized by the auto industry as a critical component: On July 3rd a paper published by leading OEMs such as

Audi, BMW, Daimler, Fiat-Chrysler, and Volkswagen, listed Control Flow Integrity (CFI) as a recommended technology for protecting safety systems against cyberattacks. Karamba Carwall is the industry-leading CFI solution, thanks to its seamless implementation and negligible performance impact.

About Karamba Security
Karamba Security provides industry-leading embedded cybersecurity solutions for connected systems. Product manufacturers in automotive, Industry 4.0, IoT, and enterprise edge rely on Karamba's automated runtime integrity software to self-protect their products against Remote Code Execution (RCE) cyberattacks with negligible performance impact. After 32 successful engagements with 17 automotive OEMs and tier 1s, product providers trust Karamba's award- winning solutions to increase their brand competitiveness and protect their customers against cyberthreats.

More information is available at www.karambasecurity.com and follow us on Twitter @KarambaSecurity

Press contacts
Idith Laga
Piabo

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